Privacy Commissioner
Te Mana Mātāpono Matatapu

Submissions received during consultation on the proposal to incorporate IPP3A into four Codes of Practice

Published on 27 March 2026

Table of Contents

Privacy Foundation submission....3
Law Association of New Zealand submission....14
Internet New Zealand submission....22
Fonterra submission....33
Hudson Gavin Martin (HGM) submission....37
Spark submission....42
Spark informal consultation....45
One NZ submission....48
ACC submission....51
Health NZ submission....58
The Royal New Zealand College of General Practitioners submission....64
Medical Council submission....67
Medical Protection Society (MPS) submission....71
Medical Protection Society (on behalf of MPS members) submission....78
Experian submission....83
Centrix Group Limited submission....85
Centrix Group Limited, informal consultation....86
Equifax informal consultation....95

Privacy Foundation NZ

15 February 2026

Privacy Act code amendments – comments from the Privacy Foundation NZ

Many thanks for the opportunity to comment on the proposed amendments to various Codes of Practice under the Privacy Act.

We have provided some general comments first, and have then provided comments on each proposed Code amendment. We hope that our suggestions are helpful for you.

1 General questions

G1 Do you agree that code amendments are desirable or needed to implement IPP3A?

Yes.

Even if IPP3A were to be unmodified, it is still useful to incorporate it into all of the more general Codes (Health, Credit Reporting, Telecommunications and Biometrics). This avoids the need for users to have to look at both the Code and the IPPs when they are considering how the privacy principles apply.

G2. Do you agree with our proposal to consider code amendments to implement IPP3A for the BPPC, CRPC, HIPC, and TIPC but not for other codes?

We agree that it is not necessary to update the unique identifier codes (Justice Sector, and Superannuation Schemes). They only modify IPP13, and the other IPPs have always simply applied as normal. It is unlikely that IPP3A would create new privacy risks or operational issues that would need to be addressed as part of the Code itself.

The same can be said in some respects of the Civil Defence Code. It is a unique type of Code (expressly focused on information sharing for national emergency management), and it does not visibly try to mirror all of the privacy privacy principles. For example, it does not modify the transparency requirements of IPP3: that principle operates as normal. It would be

somewhat odd to include IPP3A when the Code does not expressly refer to the other collection principles.

However, leaving IPP3A out of the Code of course means that it will apply in unmodified form. We wonder whether this could raise two potential problems.

First, it is important that IPP3A is not seen as raising barriers to appropriate information sharing in emergency situations. It is inherent in an emergency response that information may need to be collected from sources other than the people themselves. The policy reason for the Code is to ensure that emergency response agencies can share information for the listed, permitted purposes without having to work out whether the Privacy Act applies, at a time when they need to make decisions most urgently. Uncertainty about what is permitted could potentially delay or block valid information sharing on the ground.

Equally, though, the IPP3A exceptions should not be read so widely that they undermine the policy reasons behind IPP3A itself.

There are some specific features of emergency situations that could result in a lack of transparency, such as urgency, multi-agency sharing, practical difficulties in communication and the need to prioritise time and resourcing. But people still need to know where their information is. The only way they will find that out if they are told at or after the point of collection. It is very unlikely that people will *already* have been told that their information could be shared: in contrast with many other information sharing arrangements, IPP3A(3) will not assist.

In summary, while we agree that writing IPP3A into the Civil Defence Code itself could be difficult, we recommend that specific new guidance is developed to show how IPP3A works in practice in the context of the Code. Guidance can be built into emergency planning to both prevent risk aversion with sharing but also maximise transparency.

Examples that could usefully be included in guidance are:

- When it will not be "reasonably practicable" to notify someone (not only in obvious situations of death and injury, but also because of lack of contact details due to displacement).

- When people should be told.
  What is "reasonably practicable" in this context is open to interpretation, which is unhelpful both for affected people and responder agencies.

  We specifically recommend that OPC makes its regulatory expectations clear here. For instance, guidance could set out that agencies must inform people at the time of collection if practicable; or inform them as part of other communications with those people about the emergency response (eg in conversations when calling on people

for welfare checks); or if neither of those options is feasible due to the nature of the emergency, then inform people as soon as the emergency situation permits, but in any case not later than 20 days after the lifting of the state of national emergency (to tie with the other application timeframes in the Code).

- How to avoid notification fatigue and unnecessary duplication of resources.
  There are commonly a large number of responding agencies in an emergency, which could lead to people receiving multiple notifications. It is also unhelpful for each agency to have to spend time and effort on notification if a more streamlined approach is available. It would therefore be useful for OPC to make it clear that agencies can (and ideally should) co-ordinate their notifications (eg designate a single agency responsible for notification) provided that that notification contains all the required information about all recipients.

- Expectations around retention.
  Again, it is common for information to be shared around multiple agencies during emergencies. There are therefore heightened risks of later re-use of the information for secondary purposes. One major control is to have strong retention rules.

  Of course, while the Code does not expressly deal with it, IPP9 already applies. Disclosing agencies can (and should) include retention and destruction conditions when sharing information, and should take some subsequent steps to verify that those conditions have been met. However, it would be useful if there was a clear prompt from OPC that it expects these protections to be implemented. In the absence of any specific new requirement in the Code itself (such as an obligation to inform people about retention periods, as there is in rule 3(1)(i) of the Biometrics Processing Privacy Code), this prompt should be included in guidance.

G3. Do you agree with our proposed amendment to fix the error in clause 6(1)(c) and (d) of the Civil Defence Code?

Yes. While it is clearly a formatting error, this is a good opportunity to address it.

G4. Do you agree with our proposed approach to technical amendments and updated drafting across the codes in scope?

- Changes to rule 12 in the Codes in response to the Statutes Amendment Act 2025.
  Yes. It makes sense to update the Codes to reflect all recent legislative amendments to the Privacy Act, where applicable.

- Changes to the rule 3 headings in each code to align with the Privacy Amendment Act 2025.
  Yes. It would certainly be useful to have headings that clearly distinguish between Rule 3 and Rule 3A, as this will help users to quickly identify which Rule is applicable to particular situations. Consistency of language is also useful.

  We note in passing that the heading of IPP2/Rule 2 remains somewhat obscure, and that IPP2 also relates to 'collecting personal information from the individual concerned. The title of IPP3A might more usefully refer to 'notification'.

- Other technical changes to update language and align with terms in legislation.
  Yes. For instance, it makes sense to use this opportunity to update references to agencies where names have changed. The updated agency names would already be implied, so there is no legal problem to fix, but it avoids uncertainty for users if the Codes as up to date as possible.

G5. Do you agree with our proposed approach to implementing IPP3A?

We agree that most exceptions should be able to be incorporated without change into the Codes. More detailed comments are provided under our discussion of each Code.

G6. Although we are not currently looking at wider amendments to the codes, are there any other comments you want to provide on the codes beyond IPP3A?

Not at the moment. However, the Privacy Foundation has a major focus on potential Privacy Act reform this year, and we may have suggestions for proposed amendments to the Codes as that work progresses. If so, we will send those suggestions through to you at that time.

The rest of this submission focuses on comments on individual Codes.

2 Biometrics Processing Privacy Code ("Biometrics Code")

We agree with the proposals to include a new Rule 3A in the Biometrics Code. All the other principles are represented, even if they have not been modified, and it would be very strange to omit IPP3A. It would also make the Code much less usable: it should be as much of a one-stop shop as possible.

In addition, transparency is particularly important with biometric information (and with all more sensitive types of information). It is essential that people are clearly told who has their biometric information and what is being done with it. Of course, other rules in the Code place positive obligations on agencies to manage biometric information appropriately (for instance rules about ensuring necessity and proportionality, limiting use, or ensuring accuracy). However, this is not enough, particularly if biometric information has been collected indirectly. People cannot exercise their rights to access their biometric information or challenge what agencies are doing with it and hold them accountable unless they are told where to look or who to ask.

Specific comments on the exceptions

We agree that the Code should incorporate the following exceptions:

(a) Where people have already been told

This is an important exception, and it should be the exception that is most commonly used in practice. Having it available:

- creates incentives to give people clear and accessible information up front about where their biometric information is going, why that sharing is needed, and what will be done with the information: it supports the policy reason behind IPP3A itself.
- reduces the risk of notification fatigue for individuals
- is more efficient for agencies.

(b) Serious threat to safety

Safety is a core exception in IPP2, permitting personal information to be collected indirectly. We agree that it is foreseeable that, in at least some of those circumstances, notifying the person could in itself create safety risks (for instance in family violence or child safety situations).

(c) The exceptions under IPP3A(4)(c)

The same reasons for exempting notification in IPP3A for these circumstances appear logically to apply in the context of biometrics, despite the heightened sensitivity of that information. It is highly likely that information will be collected indirectly in those context, but the agencies concerned (eg Police) already have obligations under the Code to manage

that information in a proportionate and responsible way. Those exceptions reflect strong public interests which it is important not to disrupt.

(d) Public interest archiving

The reason for including the GLAM exception in IPP3A was because there were real practical difficulties of identifying personal information in some archival records and providing notification when the information is 'collected' by the archive repository (which may be many years after the information was originally collected by the depositing agency). It may be relatively uncommon for biometric information (as defined in the Code) to be included in archive material. However, its presence is still foreseeable enough that it makes sense to replicate the exception to prevent problems from arising.

It is particularly important to include this exception as the Code does not including the 'not reasonably practicable' exception, which archives would usually also be able to rely on.

We agree that the Code should not incorporate the following exceptions:

(a) no prejudice to individual

This is too broad and subjective an exception for biometric information (the same is potentially true for other types of highly sensitive personal information). It is not for the agency to second-guess what people may need to know. People have a stronger need than normal to be informed about where their biometric information is and what it is being used for.

(b) 'publicly available'.

This was also omitted from the Code for good reasons, and should not be available as an exception here. Again, the same need for transparency exists, even if the information was collected from a publicly available source. There need to be much stronger grounds for denying people that transparency than this broad exception would reflect.

We agree that the Code should modify the following exception:

(a) deidentified information for statistical or research use.

The OPC reasoning to limit the exception makes sense. Biometric information is, by definition, fundamental to the identity of the person even if the biometric information (eg a template) is not itself stored in a form that identifies the person. IPP3A(4)(g) appears superfluous at best and confusing at worst.

We disagree with (or are at least cautious about) the OPC proposals for the following exceptions:

(a) Prejudice the purposes of collection

On balance, it may make sense to include this exception, as it will mirror what is already set out in rule 3 (though we have similar concerns with its inclusion there) and there may be circumstances in which it would need to apply. However, we consider those circumstances should be much rarer for biometric information than they would be for other types of personal information.

As a result, we suggest that it is worth closely watching how this exception is used. The purposes for collection are already closely governed by the Code, but there is still a risk that agencies will try to define their purposes more broadly than they should. It would then be relatively easy to try to claim that notifying someone would prejudice the purposes of the collection. Agencies that have a genuine reason for not notifying someone because it would prejudice the purpose of the collection will generally be able to rely on another core public interest exception (such as maintenance of the law or safety). It would be preferable to require a more stringent exception for biometric information.

(b) Security and defence

We consider that including this exception is likely to be superfluous, and potentially confusing. If the relevant authorities are already excluded from the Biometrics Code, it is hard to see who would use this exception and for what purpose. Any applicable agency who is questioned about why they did not notify should simply be able to point to the fact they are not covered by the Code.

(c) Disclosure of trade secret or commercial position

Protecting trade secrets is an established and important legal principle, to support investment in innovation and to protect businesses from unfair competition.

However, it is unclear how notifying someone of the matters required under IPP3A could disclose a trade secret or unreasonably prejudice an agency's commercial position. For example, IPP3A does not require the agency to explain how a system works – it simply requires the agency to be open with the person about the fact and purpose of the collection.

There have been many reported cases of agencies employing biometric technologies claiming commercial confidentiality as a reason for resisting transparency (sometimes justified, sometimes not justified). Such claims can undermine the ability to hold agencies to account for the design and operation of their systems.

If OPC keeps the exception as proposed, associated guidance should make it clear that the exception will rarely apply, since the notification itself and the information provided are unlikely to undermine trade secrets or commercial positions.

The remaining proposals

We agree with OPC's remaining proposals about:

- conspicuous notice
- timing
- notice of alternatives
- commencement for new processing in line with IPP3A itself coming into force - that is 1 May 2026; or on 3 August 2026 for existing processing, to align with the Code itself coming into force for those activities.

  While agencies with existing processing may be concerned about the lack of time to adjust, there is no significant prejudice to them, as they should already have been anticipating having to comply with IPP3A and the proposals largely mirror those requirements (apart from a few exceptions now being unavailable).

3. Credit Reporting Privacy Code (Credit Code)

We consider that it is essential that IPP3A(3) is incorporated into the Credit Code. Indirect information collection is fundamental to credit reporting businesses – it is the source of nearly all the information that they hold. This is why Schedule 3 of the Code already requires credit reporters' subscriber agreements to include clear information that tells the customer that their information may be sent to a credit reporting agency.

Provided that this existing legal obligation is complied with, the exception in IPP3A(3) will apply for most transactions. The customer will (or should) already be aware that the credit reporter may have their information, and further notification at the point of collection will not be necessary.

However, we agree that the IPP3A obligation should remain on the credit reporter, not be shifted to credit providers or other subscribers. Credit reporters collect extensive amounts of often highly sensitive information about people, including information that can have a profound and lasting impact on fundamental aspects of people's lives, such as renting or buying a home, purchasing goods, setting up and running businesses, and working in certain types of positions. The fact that subscribers also have obligations is beside the point. There is simply no basis for removing the notification obligation from credit reporters. To do so would frustrate the policy behind IPP3A in one of the most important industries that it would apply to.

Nor are there practical problems for credit reporters with including it. If the system is functioning correctly - which is largely in the credit reporter's control – IPP3A will place no (or very little) additional burden on them.

We note that credit reporters also have to provide annual assurance to OPC about the matters listed in schedule 7. One of the items on the list is that they need to provide assurance that subscriber agreements that meet the requirements of schedule 3 are in place

before disclosing credit information. We suggest that OPC could usefully require specific assurance (at least initially, and periodically thereafter) about whether the information provided by subscribers meets the standards expected under IPP3A. This level of monitoring would provide an additional layer of confidence that people are aware of where their information is sent and what is being done with it.

We have no specific comments on any of the other aspects of the proposals.

4. Health Information Privacy Code

We support the introduction of a dedicated rule 3A into the Health Information Privacy Code. Given multidisciplinary care, referral pathways, shared care arrangements and data-linkage in health services, indirect flows of information are routine, and sharing and collection can occur many times across an episode of care. Given that much of this may be invisible to health consumers, making information flows more transparent is essential to patient trust, informed participation in care, and appropriate health-research ethics practices.

It is appropriate and sensible to align the wording and applicable exceptions with the existing HIPC Rule 3 and IPP3A wording. This is particularly relevant to rule 3A(4)€ in the health context.

We consider that the draft HIPC amendments are broadly workable, provided that the final code is accompanied by robust, health-specific guidance that centres on consumer perspectives and the particular cultural and ethical issues inherent in indirect health information collections. The effectiveness of Rule 3A in practice will require clear, pragmatic guidance to support a consistent and workable implementation by health agencies.

We are strongly supportive of the OPC issuing standalone health sector guidance for rule 3A, to ensure agencies can operationalise requirements effectively and efficiently. Suggestions for inclusion in the guidance are:

- Provide clear examples of common indirect collection scenarios in the health sector (e.g referrals, shared electronic records, information flows to Te Whatu Ora | Health New Zealand), advice when rule 3A applies and when exceptions could be considered.
- To illustrate what “reasonable steps” and “reasonably practicable” look like in common health sector workflows (for example referrals, virtual care, shared-care platforms, outsourced services), with a strong emphasis on patient-centred design rather than mere technical feasibility.

- Advice as to how agencies should apply rule 3A(3) proportionately, and what may be required in instances where there is high frequency, time sensitive sharing required across multiple agencies and it may be unclear when an individual "is already aware".
- How agencies should interpret "prejudice" under rule 3A(4)(a).
- Details around representatives should be aligned with any existing guidance from the Health and Disability Commissioner and speak to capacity being reassessed over time so that agencies continue to consider when direct notification.
- Encouraging agencies to co-design notices and notification with consumers and health workers, including Māori, Pasifika, disabled people, tāngata whaikaha Māori and frequent health service users to ensure appropriate rule 3A implementation. Examples of good practice notification in common health settings/context would be helpful, referencing options around layered 10rivacy notices, consent conversations and point of care discussion.

With respect to rule 2(2)(a) collection of information for family or genetic history, we acknowledge the practical rationale for aligning rule 3A with rule 2 so that health agencies need not notify every family member whose information is collected indirectly when assembling a family or genetic history from a patient. We accept that, without such an exception, some clinically important family-history collection could become operationally unworkable.

However, from both a health-consumer and human-rights perspective, this is one of the most ethically and culturally sensitive areas of indirect collection, touching directly on whakapapa, kinship, and inter-generational interests. We are particularly concerned about:

- the potential for family-history or genetic information to be used in ways that affect relatives who have had no interaction with the health agency; and
- conflicts between Western individual-consent models and collective or whānau-based approaches to decision-making.

We therefore recommend that the OPC:

1. Treat this as a provisional exception that must be accompanied by:

- clear guidance on the limited scope of the exception and appropriate uses of family/genetic information; and
- strong expectations that agencies handle such information with heightened care, including conservative reuse and disclosure practices.

2. The commitment to dedicated engagement with Māori, Pacific peoples and other communities whose concepts of identity and family may be particularly impacted, with a view to revisiting this exception and/or introducing complementary

obligations (for example, “collective” transparency obligations or whānau-level engagement) in a future HIPC review.

5. Telecommunications Information Privacy Code

As with the other broad Codes, we agree that IPP3A should be brought into the Code itself, to bring all relevant provisions together.

We also agree that Schedule 4 should remain unaffected. That schedule already contains provisions requiring notification that information was collected and shared. It is important that those transparency requirements are not watered down in any way by the introduction of a broader range of exceptions.

Unfortunately, due to resourcing constraints, we have not managed to consider the specific proposals for this Code in any more detail at this time. However, we are available for further discussions if this would be useful for you.

Conclusion

We hope that our comments are helpful. Please feel free to contact us if you have any queries or would like to discuss anything further.

Katrine Evans, Chair, Privacy Foundation NZ Inc

The Law Association OF NEW ZEALAND

Vero Centre
Level 18
48 Shortland Street
Auckland City 1010
New Zealand
PO Box 58
1010 Auckland
09 303 5270
thelawassociation.nz

Privacy code of practices - Incorporating Information Privacy Principle 3A (IPP3A)

Submissions on behalf of The Law Association of New Zealand by the Technology and Law Committee

The views represented in this submission are not necessarily representative of the views of all TLANZ members but are those of individual TLANZ members or TLANZ committees who have responded to the consultation.

1. INTRODUCTION

1.1. The Law Association of New Zealand (TLANZ) is an independent membership organisation for the New Zealand legal profession with more than 9,000 members. TLANZ maintains expert law committees that support legal review and policy advocacy on important issues.

1.2. This submission is made by the Technology and Law Committee of The Law Association of New Zealand (TLANZ). The Committee comprises legal practitioners with expertise in privacy, technology law, data governance, and regulatory compliance. Members advise both public and private sector organisations on privacy obligations and regularly engage with emerging issues arising from digital technologies and artificial intelligence (AI).

1.3. The Technology and Law Committee of The Law Association of New Zealand (TLANZ) welcomes the opportunity to comment on the proposed amendments to the:

- Biometric Processing Privacy Code 2020 (BPPC)
- Health Information Privacy Code 2020 (HIPC)
- Telecommunications Information Privacy Code 2020 (TIPC)
- Credit Reporting Privacy Code 2020 (CRPC)
- Civil Defence National Emergencies (Information Sharing) Code 2020

to incorporate or align with Information Privacy Principle 3A (IPP3A).

1.4. The Committee supports, in principle, the incorporation of Information Privacy Principle 3A (IPP3A) across the relevant Codes of Practice. Enhancing transparency around indirect collection is consistent with the underlying purposes of the Privacy Act 2020 and reflects modern data ecosystems where personal information is frequently obtained from third parties or derived through digital systems rather than collected directly from individuals.

1.5. However, the Committee considers that the proposed amendments do not yet adequately address the realities of AI-driven data collection, analysis, and reuse. AI systems fundamentally alter how personal information is aggregated, inferred, and deployed. Without explicit safeguards, the transparency objectives of IPP3A risk being undermined in practice.

2. EXECUTIVE SUMMARY

2.1. The Technology and Law Committee of The Law Association of New Zealand (TLANZ) supports, in principle, the proposed amendments aligning the Biometric, Health, Telecommunications, Credit Reporting, and Civil Defence Codes with Information Privacy Principle 3A (IPP3A). Strengthening notification where personal information is collected indirectly promotes transparency, trust, and informed participation in digital environments.

2.2. The Committee's key messages are:

- Notification exceptions must be applied cautiously, particularly for sensitive information such as biometric and health data.

- The “not reasonably practicable” exception should set a high threshold in sensitive contexts.
- Modern data practices increasingly involve AI and advanced analytics, which heighten the importance of transparency.
- Clear guidance is desirable on the commercial prejudice exception in the Biometric Code.
- In emergency contexts, purpose limitation, data minimisation, and lifecycle controls remain critical to maintaining public trust.

2.3. Overall, the Committee considers the proposed reforms constructive and encourages continued attention to transparency, proportionality, and technological accountability so the privacy framework remains credible and fit for a data-intensive environment.

3. SUBMISSIONS

3.1. *General Observations on IPP3A and Exceptions*

3.1.1. Alignment between the Codes and IPP3A promotes coherence across the privacy framework and reduces fragmentation in standards. The Committee supports this harmonisation. However, the effectiveness of IPP3A depends on how its exceptions operate in practice. If applied broadly, there is a risk that transparency objectives may be weakened. This is especially significant where sensitive information is concerned.

3.1.2. The Committee endorses a cautious approach to the “not reasonably practicable” exception. Where information is inherently sensitive, individuals’ expectations of transparency are correspondingly higher, and agencies should meet a high threshold before relying on this exception.

3.1.3. The Committee also notes the growing prevalence of AI and automated analytics in personal information ecosystems. While the amendments are not AI-specific, AI-enabled processing can change the risk profile of personal information through large-scale aggregation, inference, and reuse. In such contexts, transparency becomes more, not less, important. The Committee encourages continued attention in guidance and future reform to how privacy principles operate in AI-enabled environments.

3.2. *Overarching Position on AI and Indirect Collection*

3.2.1. The Committee’s central concern is that the proposed amendments are largely technologically neutral, at a time when neutrality may no longer be sufficient. AI systems are not merely another processing tool; they are capable of large-scale aggregation, inference, profiling, and secondary use that individuals cannot reasonably anticipate.

3.2.2. The Committee therefore submits that AI-enabled collection, analysis, or reuse of personal information should not benefit from broad notification exceptions that were originally designed for more conventional forms of data handling.

3.2.3. The “not reasonably practicable” exception in IPP3A(4)(e) should be interpreted narrowly where AI is involved, particularly where sensitive information is concerned. The Privacy Commissioner’s existing guidance already recognises that higher thresholds apply to sensitive information. Biometric and health information sit at the highest end of sensitivity and should attract correspondingly strong expectations of notification.

3.2.4. In practical terms, AI systems often operate precisely because large datasets are pooled and analysed at scale. Allowing agencies to rely on practicability exceptions as a norm would undermine the default privacy premise of transparency in situations where it is most needed.

3.2.5. The Committee is concerned that the Codes are presently silent on AI, despite AI-driven analytics being a significant driver of privacy risk and a common factor in major data incidents. Silence in this area may inadvertently signal that existing exceptions apply unchanged to AI environments.

3.3. *Transparency and Meaningful Awareness*

3.3.1. The Committee considers that meaningful transparency requires more than a generic notice that information may be used or shared. Where personal information may be processed by or fed into AI systems, individuals should be informed of this fact in clear and accessible terms.

3.3.2. At a minimum, agencies should disclose:

- that AI tools are used in processing or analysing the information;
- the general purpose for which AI is used; and
- whether the AI involves external platforms or service providers.

3.3.3. This is not to require disclosure of proprietary algorithms, but rather to ensure individuals understand the nature of processing that affects them. Without this, consent and awareness risk becoming purely formal.

3.3.4. The Committee also supports the concept, raised in member feedback, that individuals should have a genuine ability to opt out of AI-driven uses where feasible and where the AI use is not strictly necessary for a statutory function. Even where opt-out is not possible, transparency remains essential.

3.4. *Biometric Processing Privacy Code 2020 (BPPC)*

3.4.1. The Committee agrees that aligning the BPPC with IPP3A is appropriate. However, biometric information presents uniquely high risks. Biometric data is persistent, difficult to change, and increasingly linked to automated identification and tracking technologies.

3.4.2. The Committee submits that notification exceptions should apply only in truly limited circumstances where biometric data is concerned. In particular, reliance on “not reasonably practicable” should be rare, given the sensitivity and potential long-term consequences of biometric misuse.

3.4.3. The Committee also endorses the request for further guidance on what constitutes "unreasonable prejudice to a commercial position" under Rule 3A(9)(b). Without clarification, there is a risk this exception could be invoked too broadly. Commercial sensitivity should not become a routine basis for limiting transparency around biometric data practices.

3.4.4. Where biometric data is processed using AI-enabled systems, the Committee considers that strong transparency expectations should apply, including disclosure that automated recognition or matching technologies are involved.

3.5. ***Health Information Privacy Code 2020 (HIPC)***

3.5.1. The Committee supports alignment of HIPC with IPP3A.

3.5.2. Health information sits at the highest end of sensitivity. Individuals have strong and reasonable expectations about how their health data is collected and used. The Committee strongly supports the view that notification exceptions should be interpreted restrictively in the health context. The threshold for impracticability should be high. Routine or system-driven indirect collection should not automatically qualify for exceptions.

3.5.3. Within the broader category of health information, mental health information and disability-related information warrant particular attention. Such information often carries social stigma, risks of discrimination, and significant implications for employment, insurance, housing, and social participation. The misuse or unexpected secondary use of this data can have enduring consequences beyond immediate clinical contexts.

3.5.4. The Committee considers that when assessing whether notification is "not reasonably practicable", agencies must take into account the heightened vulnerability of individuals whose information concerns mental health conditions, neurodiversity, intellectual disability, or psychosocial disability. In these contexts, transparency is not merely procedural; it is central to respecting dignity and autonomy.

3.5.5. The Committee also notes that individuals receiving mental health services or living with certain disabilities may experience barriers to understanding complex privacy notices. Accessible and comprehensible notification is therefore particularly important. Agencies should consider whether notice mechanisms are genuinely accessible, including through plain language, supported decision-making frameworks, or alternative communication formats where appropriate.

3.5.6. Health data practices can affect dignity, autonomy, and wellbeing. Transparency plays a central role in maintaining trust in the health system. The Committee agrees that the threshold for what is "not reasonably practicable" should be high in this context. Health data environments are increasingly digital and may involve predictive analytics, triage systems, and diagnostic support tools. AI use in mental health and disability contexts raises additional ethical and privacy considerations. Predictive risk scoring, behavioural profiling, and automated

triage tools may influence access to care or support services. Where health information is used in AI systems beyond direct clinical care delivery, individuals should be made aware in general terms.

3.5.7. The Committee further notes that AI systems trained on health datasets may embed historical bias, particularly in relation to disability or mental health. Transparency around AI involvement assists not only individual awareness but also broader accountability in high-impact decision-making environments. Given the sensitivity and potential downstream impact of mental health and disability information, the Committee considers that reliance on notification exceptions should be rare and clearly justified in these contexts.

3.5.8. AI use generally in health contexts, including predictive analytics or diagnostic support tools, and raises additional ethical and privacy considerations. The Committee considers that, where health information may be used in AI systems beyond direct care delivery, individuals should be made aware in general terms.

3.6. *Telecommunications Information Privacy Code 2020 (TIPC)*

3.6.1. The Committee supports the addition of rule 3A to TIPC. Telecommunications data can be highly revealing, particularly when aggregated or analysed at scale. It may disclose patterns of movement, association, and behaviour. Transparency expectations are, therefore, correspondingly high.

3.6.2. Telecommunications data is increasingly used in analytical and modelling contexts. The Committee's concern is that notification exceptions could unintentionally obscure significant uses of personal information. Exceptions should therefore be applied carefully so that individuals are not left unaware of material data uses.

3.6.3. The committee also notes that telecommunications data is particularly rich in behavioural and locational insights. When combined with AI analytics, such data can reveal highly detailed patterns about individuals' lives.

3.6.4. The Committee considers that explicit recognition of AI-related processing risks would strengthen the Code. Telecommunications providers are major adopters of AI for network management, fraud detection, and customer analytics. These practices heighten the importance of transparency.

3.6.5. Consumers should not be left unaware that their data may feed into AI-driven systems. Clear notice promotes trust and aligns with the Act's emphasis on openness.

3.7. *Credit Reporting Privacy Code 2020 (CRPC)*

3.7.1. The Committee agrees with incorporating IPP3A into the CRPC.

3.7.2. Credit reporting already relies heavily on automated and algorithmic processing. Such processing can materially affect individuals' access to credit, housing, and

services. Transparency in this context is closely linked to fairness and accountability.

3.7.3. Individuals should not be left unaware of how their information is assessed and used, particularly where automated tools are involved. Meaningful notification supports both procedural fairness and confidence in the credit reporting system.

3.7.4. Credit information already has significant downstream effects on individuals' financial lives. AI-driven credit scoring and risk assessment tools are becoming more common. While these may improve efficiency, they can also introduce opacity and bias. The Committee considers that individuals should not be unaware that automated or AI-assisted profiling may occur in credit contexts.

3.7.5. Transparency in this domain supports fairness and aligns with principles of responsible data use.

3.8. ***Civil Defence National Emergencies (Information Sharing) Code 2020***

3.8.1. The Committee recognises the distinct role of the Civil Defence Code in facilitating timely information sharing during a declared national emergency. In such contexts, a calibrated shift in the balance between privacy and public interest is both expected and, in many cases, necessary.

3.8.2. The Committee does not oppose the recent technical amendment clarifying disclosure to persons responsible for an individual. This is a practical refinement in emergency situations. Emergency management is increasingly data-driven and technologically mediated. Agencies may rely on predictive analytics, geolocation data, and digital platforms to coordinate responses. These developments can enhance effectiveness but also raise questions of proportionality and oversight.

3.8.3. The Committee emphasises that the concept of a defined "permitted purpose" must remain central and interpreted strictly so that emergency information sharing does not extend beyond its intended scope. Privacy risks in emergency contexts often arise from retention and secondary use rather than initial collection. Time-bound retention, secure handling, and deletion or de-identification once information is no longer required are important safeguards.

3.8.4. Maintaining public trust is integral to effective emergency response. Even where contemporaneous notification is impracticable, retrospective transparency about how information was used can support accountability and confidence.

4. CONCLUSION

4.1. The Committee supports the overall direction of strengthening transparency around indirect collection. However, modern data environments require explicit recognition of AI-related risks. Without this, there is a real possibility that notification exceptions will be stretched in precisely those contexts where individuals most need awareness.

4.2. The Committee encourages the Privacy Commissioner to:

- emphasise narrow interpretation of exceptions for sensitive data;
- provide guidance on AI-related transparency expectations; and
- reinforce that technological complexity does not diminish accountability.

4.3. As personal information ecosystems become more data-intensive and automated, transparency and purpose limitation remain central to maintaining public trust.

4.4. We are available to discuss our submissions, if required. Should clarification be required with regards to any matters raised, please contact Moira McFarland, the TLANZ Committee Executive at [redacted]

5. ACKNOWLEDGMENTS

5.1. The Committee acknowledges the contributions to the submissions by Amy Kingston-Turner and Lloyd Gallagher.

Ngā mihi

Lloyd Gallagher
Convenor
TLANZ Technology and Law Committee

13 February 2026

Submission on "Biometric Processing Code 2025 (BPPC) Amendments"

Office of the Privacy Commissioner

Introduction

Who we are and what we stand for

1. InternetNZ | Ipurangi Aotearoa operates the .nz domain space. We ensure all domain names ending with .nz are available for people and businesses in Aotearoa to function and thrive online. InternetNZ is committed to ensuring that our digital environment remains open, secure, inclusive, and resilient for all.

2. We are a not-for-profit organisation, and the money we receive from .nz domain names goes back into the community. We provide grants, help to fund other organisations, and advocate for an accessible and safe Internet that benefits everyone in Aotearoa.

3. You can read more about our work here.

This Submission

Summary

4. We welcome this opportunity to submit our feedback on the Biometric Processing Code 2025 (BPPC) Amendments consultation document.

5. In general, we support the policy intent to simplify the requirements of the new changes within this single document, which is more likely to lead to administrative efficiency and compliance.

6. In this submission, we highlight concerns regarding the rationale for certain proposals to shape the final Code. Key considerations include how the Code can prevent misuse of biometric information by criminals, unauthorised commercialisation by online platforms, its relationship with other laws, and how it can uphold fundamental human rights and privacy protections.

General Comments about Biometric Data Online

7. First, it is important to recognise that biometric information has particular risks as a form of personal information as it is fixed and unique to the person concerned, and it may be shared and misused in ways that an individual may not be aware of or able to control, which could result in significant harm, particularly where access is from an unknown third party.

8. We note that the Office of the Victorian Information Commissioner has outlined the following privacy challenges with the collection of biometric information:
   - Function creep
   - Covert collection
   - Secondary information
   - Consent
   - Other challenges, e.g. impacting an individual's sense of self.

   InternetNZ agrees with this framing. These challenges directly mirror the risks we see emerging in the Aotearoa online context, particularly regarding function creep and the covert collection of biometric data via third-party scripts embedded in websites.

9. Many online platforms and search engines have adopted data-driven economic models that rely on data and digital surveillance to deliver targeted advertising and predictive marketing to users. Biometric data, which may include the ability to identify a person's age, medical conditions, ethnicity, voice, and gender, will fall within this marketable commodity. And arguably, it will help with the design of targeted advertisements and engaging content that capture users' attention and maintain participation on the platform (enabling further data collection).

10. Embedding human rights and privacy rights into the governance, collection and use of this data is particularly important in a time when technology capability is developing rapidly. This is particularly important where we lack the legislative and programmatic infrastructure to ensure platforms are transparent and accountable to an independent regulator - infrastructure that exists in other jurisdictions (e.g. the EU, UK and Australia). For example, biometric information could be easily adopted by AI capabilities on a platform to produce convincing deep fakes and other forms of disinformation, as seen in the recent case of Grok on X. This is pertinent given Parliament's consideration of two member Bills - on deep fakes and a social media ban for under 16 year olds - both of which potentially relate to the collection and use of biometric information (e.g. through the creation and detection of deep fakes, or for assessing the age of individual users).

11. As the operator of the .nz namespace, InternetNZ has an interest in how identity and age are verified online. Proposals for mandatory age verification or deepfake detection necessarily rely on the types of biometric processing this Code seeks to regulate. It is vital that the technical standards underpinning the architecture of the Internet are not undermined by legislation, and that users who engage with online services have their data protected adequately.

Rule by Rule Analysis

No notification required where an individual has already been made aware of the

indirect collection – IPP3A(3)

OPC Proposal: *We are proposing rule 3A would bring in the general exception under IPP3A(3) which applies where an individual has already been made aware of the specific indirect collection. We think this is consistent, clear, and balanced; and is likely to be a commonly relied upon exception.*

InternetNZ Comment:

12. It is important that the original "awareness raising" was made in a clear and accessible way - ideally, this would actually be informed consent.

13. Accessibility is a frequent problem in an online environment, where privacy terms are included and buried within a broader set of terms and conditions, which must be accepted before a person can use an app, access an updated version, or become a platform user. The default in this situation is for people to unwittingly accept the indirect collection without a clear idea of the implications of what they are agreeing to, if they are asked for permission at all. For example, this study (published in 2023) examined ethical concerns about social media privacy policies and whether users had the ability to comprehend their consent actions. It cited a number of previous studies that showed a lack of capacity, and in their research found that:

> "younger users or those with lower reading ages lack the ability to comprehend their consent actions for social media privacy policies. Between 2005 when Facebook launched, to 2023 it has updated its privacy policy 24 times. The first version was 1,000 words and has grown to 11,476 in 2023, albeit with increased headings and links to 'learn more'. In some years the policy had several updates, due in part to negative users' reactions and legal obligations (Newcomb, Citation 2018)… users of all ages may fail to grasp the implications for data usage as the details are contained within lengthy documents that are at best, *fairly difficult to read*, requiring 18 to 48 minutes to review, at average reading speeds. Besides the length of the policies, this paper has shown that social media platforms present policies where the information is incomprehensible to many users (e.g. 'pursuant to binding contractual obligations')."

14. In the context of the sensitivity of biometric information and privacy in the online environment, the proposal in the discussion document raises questions about:
    - Consent & Revocation: How can a person decline consent following notification, or revoke it later?
    - Access & Correction: How can a person access or correct indirectly held information?
    - Third Parties: Will individuals be told exactly who the third party is, and what obligations they have?
    - Data Chains: Could the information be shared with a fourth or fifth party and what the obligations are?
    - Function Creep: How will the OPC monitor the risk of third parties repurposing this data?

- Commercialisation: What protections exist against the commercial sale of indirectly collected biometric data?"
- Data Security: What protections secure indirectly collected information against misuse and theft? The Office of the Victorian Information Commissioner has advised on the risks of identity theft from biometric information.
- Scope: Does the proposal apply where websites use third-party verification processes, such as for security or age verification?

15. An individual should have an ongoing right and easy access to decline the collection, storage, or sharing of biometric information, including indirect collection. This will be assisted by more than one notice and in a commercial setting, there could be a requirement to, alongside the initial very clear and accessible notification, be simple, ongoing access to that notification that sits as a term and condition on the website in an easily accessible format - e.g. "How is my information used and who is it shared with" in the FAQs (if such a requirement does not already exist).

No prejudice to the individual – IPP3A(4)(a)

OPC Proposal: *We do not propose to include this exception in the BPPC as the equivalent exception in IPP3 was not carried through into rule 3 of the BPPC*

InternetNZ Comment:

16. It is unclear from the consultation document what the policy rationale was for not including the equivalent exception, but releasing biometric information is potentially more serious. The two examples provided in the Guidance on IPP3A issued by OPC include:

> Exception may apply:
> • You're collecting emergency contact information from an employee and can reasonably presume that the employee has an existing relationship with their emergency contact and has made them aware that they are their emergency contact.
>
> Exception would not apply:
> • You're collecting loyalty card information to create shopping profiles of individuals and generate targeted ads, for marketing purposes.

17. There may be edge cases where sharing does not result in prejudice (e.g. an employer providing information to an employee's doctor). However, given the immutable nature of biometric data, we believe the Code should err on the side of caution and require a higher standard of justification.

Information is publicly available – IPP3A(4)(b)

OPC Proposal: *We do not propose to include this exception in the BPPC as the equivalent exception in IPP3 was not carried through into rule 3 of the BPPC.*

InternetNZ Comment:

18. It is unclear from the consultation document what the policy rationale was for not carrying this over. In the Guidance on IPP3A issued by OPC, these two examples are given for what would / would not fall within this exemption:

    Exception may apply:
    • You are collecting personal information from a publication such as a book, newspaper, or public register.
    • You are collecting personal information from a website or public social media page.

    Exception would not apply:
    • You are collecting personal information from social media that requires you to have additional permission to view (such as being a friend or follower of a private social media account).

19. The public availability of biometric information is arguably more sensitive and subject to misuse - e.g. through AI, deep fakes, so additional protections may be justified.

Non-compliance is necessary – IPP3A(4)(c)

OPC Proposal: *We propose to include this exception in the BPPC as it is consistent with IPP3A and rule 3.*

InternetNZ Comment:

20. These are the examples given in the OPC Guidance:

    Exception may apply:
    • A public sector agency is investigating an offence and needs to collect information about a person from someone else to adequately investigate the offence, **and the agency has followed all other relevant laws that apply to gathering evidence.** It's important to note that collection must still be allowed under IPP2, even when relying on this exception.

    Exception would not apply:
    • If you are not a public sector agency.

    Note: Private sector agencies wanting to collect information about a person from someone else to do their own investigation of suspected fraud may be able to rely on other exceptions under IPP3A. For example, if telling the individual would prejudice the purpose of the collection.

21. There are two important parts to this exception:
    - That it only applies to public service agencies (and we note that SOEs and CRIs with commercial functions are outside this definition in the Public Services Act 2020); and
    - That agencies have otherwise followed the laws of evidence (and we assume surveillance is covered by this).

22. We have two questions:
    - Are there other administrative law, criminal law, procedural or substantial aspects that should also be considered here?
    - Will this information be included in the IDI or otherwise shared between public sector agencies - and what additional notifications or protections are in place in this situation?

Compliance would prejudice the purposes of collection – IPP3A(4)(d)

OPC Proposal: *We propose to include this exception in the BPPC as it is consistent with IPP3A and rule 3.*

InternetNZ Comment:

23. These are the examples given in the OPC Guidance:

    Exception may apply:
    • You are collecting personal information for a fraud investigation and notifying the person concerned would undermine your investigation.

    Exception would not apply:
    • It is less practical for you to notify the person concerned, so you don't want to.
    • You're worried about losing or upsetting the customer, so you don't want to notify.

24. Notwithstanding the clear exceptions provided in the Guidance, shouldn't there be a higher standard for biometric information? Although fraud is a clear-cut case, we think either a tighter definition or further guidance would be required to prevent misuse.

Compliance is not reasonably practicable in the circumstances – IPP3A(4)(e)

OPC Proposal: *We are not proposing to include the IPP3A 'not reasonably practicable' exception in BPPC rule 3A. This is because the same exception has not been incorporated into rule 3 of the BPPC, to reflect the sensitivity of biometric information. We think that where an agency is indirectly collecting biometric information, this is best supported by the 3A(3) requirement which requires steps to make the individual concerned aware. We further believe there could be regulatory confusion if rule 3A includes a 'not reasonably practicable' exception*

where rule 3 does not, and that agencies which are meeting their rule 3 obligations will also be able to comply with rule 3A.

InternetNZ Comment:

25. What happens if it is not possible, though? Are there minimum steps that should be covered by this?

Serious threat to health or safety – IPP3A(4)(f)

OPC Proposal: *We propose to include this exception in the BPPC. We can see use cases where this exception might be relevant (e.g. to prevent notification to an individual whose biometric information is shared where that person may cause harm to another person or public health).*

InternetNZ Comment:

26. This appears to be fine, justified on risk.

De-identified or statistical and research purposes – IPP3A(4)(g)

OPC Proposal: *We are proposing to include this exception, but to narrow it to the use of statistical or research purposes that will not be published in a form that could reasonably be expected to identify the individual concerned. This is narrower than IPP3A(4)(g), which includes an exception where the information will not be used in a form in which the individual concerned is identified. This is because biometric information relating to a particular individual will identify them.*

InternetNZ Comment:

27. Good proposal.

Public interest archiving – IPP3A(5)

OPC Proposal: *We are proposing to include an exception based on IPP3A(5) into the BPPC. This exception relates largely to the GLAM1 sector but applies more broadly to agencies that collect personal information for the purpose of determining whether the information is of enduring value for general public interest and should be archived for public reference, study, or exhibition. We believe there are potential use-cases for biometric processing in the GLAM and archiving in the public interest context. For example, where agencies are using biometric processing in working with archived images or recordings of people.*

InternetNZ Comment:

28. This appears to be fine.

- **Security and defence – IPP3A(6)**

OPC Proposal: *We are proposing to include this exception because the BPPC is not sector-specific but applies to biometric information collected for biometric processing across all sectors, and we could see hypothetical use cases where this exception would be relevant. However, as intelligence and security agencies are excluded from IPP3A and from the BPPC, we are interested in hearing from stakeholders on whether there are use-cases and whether this exception is needed.*

InternetNZ Comment:

29. These agencies are regulated by other legislation, so you would want to ensure that what is detailed in the Code is not intended or interpreted as providing justification for undermining that framework. It would not be in the public interest for this exception to be a workaround or cover gaps that are not otherwise authorised (in the same way that law enforcement have to comply with evidence law).

Disclosure of trade secret or prejudice commercial position – IPP3A(7)

OPC Proposal: We propose to include this exception in the BPPC. Similar to our proposed approach for IPP3A(6), given the BPPC is not sector-specific, we are keen to hear how IPP3A(7) could apply in the BPPC context.

InternetNZ Comment:

30. This could raise potential intellectual property issues - e.g. AI-generated material that uses that person's biometric information. Informed, accessible, and ongoing consent should be required for the collection of someone's biometric information.

Conspicuous notice – rule 3(3)(b)

OPC Proposal: *In the biometrics context, a sufficiently clear and detailed conspicuous notice for rule 3 purposes may also satisfy the requirements of the IPP3A(3) exception we propose to include. We are proposing to align this rule 3A exception with the existing language under rule 3(3)(b). We believe it is important to explicitly state that the clear and conspicuous communication needs to tell the individual which agencies would indirectly collect biometric information to fit within this exception.*

InternetNZ Comment:

31. This appears to be fine. As outlined above, a person should also be informed about their rights in relation to the indirectly collected information, how to contact those people/organisations, etc.

Timing of notification

OPC Proposal: *We are proposing to align the timing to existing requirements in BPPC rule 3. Timing in IPP3 requirements is "as soon as reasonably practicable" if not before / at time of*

collection, and in rule 3 of the BPPC there is this requirement:

"(4) Any steps to ensure the individual's awareness of the other matters set out in subrule (1) must be taken before the biometric information is collected or, if that is not practicable, as soon as practicable after the biometric information is collected."

InternetNZ Comment:

32. This appears to be fine.

Notice of alternatives – rule 3(c)

OPC Proposal: *We think that it makes sense to include the requirement to notify individuals of any alternatives available to them if the agency indirectly collecting their biometric information will conduct biometric processing of that biometric information. This requirement does not mean that an agency needs to provide an alternative. It only requires them to advise the individual whether or not there is an alternative available. To exercise any alternative options to the processing of biometric information indirectly collected, the person needs to know about it.*

InternetNZ Comment:

33. We are aware that commercial entities, such as supermarkets, are currently collecting biometric information about customers. Given the intersecting problems of supermarket monopoly in New Zealand and the sensitivity of biometric data, we are concerned that the lack of alternatives means a person has no choice but to have their data collected if they want to buy food or other essential products. This is particularly true in small towns, where there may be only one or two supermarket operators. There needs to be stronger protections for the right to privacy than what is proposed.

34. Genuine choice requires a viable alternative. European regulators have required platforms to offer genuine (data-free) choices under Article 5(2) of the Digital Markets Act. We submit that the OPC should consider similar guidance for apliciable New Zealand entities. If a business or platform offers no alternative to biometric processing, the 'notice of alternatives' requirement is rendered meaninglessGenuine choice requires a viable alternative.

Information rule 3A will apply to – rule 3A(10)

OPC Proposal: *The BPPC provides a staggered commencement date, depending on whether an agency was undertaking biometric processing on 3 November 2025. This approach has been followed for the amendment, which means the new rule 3A, and the information it relates to, will also apply at different times, depending on when the BPPC applies to that agency's activity.*

InternetNZ Comment:

35. It is unclear how much time individual organisations may need to adjust their policies and procedures to comply with the new requirements.

Next Steps

36. We are happy to meet if you have any questions about our submission, please contact us at policy@internetnz.net.nz.

Fonterra Submission: Draft Guidance on IPP3A

13 February 2026

Introduction

Fonterra welcomes the opportunity to comment on the proposed amendments to implement IPP3A in codes of practice.

Fonterra is a New Zealand farmer owned dairy co-operative, built by generations of farmers, for farmers. We are more than just a processor – we are an extension of their farming business, partnering alongside farmers to provide industry-leading support where it matters most. Fonterra has a significant presence in New Zealand, employing more than 10,500 people across our network of 24 manufacturing sites, Farm Source retail stores and offices.

At Fonterra, consistently ensuring we do what is right to protect the privacy of the individuals we engage with is fundamental to our integrity. This includes respecting the privacy of our employees, farmer shareholders, customers, suppliers, vendors, and all other stakeholders. We ensure that the personal information collected and processed as part of those relationships is managed in accordance with applicable privacy legislation and regulatory requirements in the jurisdictions in which we operate.

Fonterra's commitment to privacy is set out in a dedicated section of our Code of Business Conduct. We also have a Group Privacy Policy and a Group Privacy Standard, detailing our privacy obligations and how these should be met. Our Privacy Statements also reiterate our privacy commitments and provide information to individuals regarding our processing of their personal information.

Fonterra supports the intention of IPP3A, which has the stated aim to bolster transparency about how personal information is collected in New Zealand.

We agree with the intent in which IPP3A seeks to shed light on potential "invisible" processing of personal information, which may not necessarily be clearly set out in an agency's privacy statement. We also support the provisions in IPP3A, when enacted, will align the New Zealand Privacy Act 2020 more generally with privacy laws of other jurisdictions. We understand the intention is to add a new rule 3A to codes of practice issued under the Privacy Act 2020 to implement IPP3A and align with the existing rules in each code, and including relevant exceptions.

Fonterra has reviewed the information papers, amendments and marked-up changes to the codes. Our comments are limited to the Biometrics Processing Privacy Code and proposed changes only.

As stated in our previous submission on IPP3A, Fonterra considers the proposed approach may result in a significant increase in the number of notifications an individual receives and consequently may fail to have the intended impact of increasing visibility of "invisible" processing of personal information. The proposed approach also has considerable compliance costs for businesses, and the requirements may be complex to understand and implement. Fonterra suggests the OPC should consider alternative approaches that will

streamline compliance for agencies where possible. We also suggest that more guidance is needed for New Zealand businesses to understand how to appropriately comply with their requirements under these new rules.

Multiple deadlines for compliance may create confusion

The BPPC has two potential dates on which it may come into force - 3 November 2025 for new uses of biometrics within a business, and 3 August 2026 for existing uses of biometrics.

IPP3A and its proposed amendments to the Codes will come into force on 1 May 2026.

The proposed date is 1 May 2026 for IPP3A to enter into force.

For existing uses of biometric information, the grace period for the BPPC will expire on 3 August 2026, which means businesses must meet the requirements under IPP3A first and then adjust to the similar, but not the same BPPC Rule 3A.

This creates a dual milestone. Depending on how businesses are structured and run, this could cause complexity and mean a two-phased approach of updating notices and SOPs. New Zealand's business landscape is comprised of 97% small businesses, mostly 20 or fewer employees. These small businesses are required to understand and comply with the Privacy Act 2020, its additions and amendments, yet are unlikely to have a dedicated privacy function. To mitigate the likelihood of confusion, we believe it would be beneficial to streamline the compliance deadlines wherever possible.

We understand that it may not be feasible at this time to alter previously communicated dates for compliance, however we suggest a grace period across all functions until 3 August 2026 - by which time all agencies should be compliant with:

1. IPP3A;
2. Rule 3A in the Biometric Processing Privacy Code; and
3. The Biometric Processing Privacy Code.

In addition, we note in the proposed changes to Rule 3A(1)(10) which specifies when Rule 3A should apply, there appears to be a typo in the marked-up document provided for review and consultation. It is our understanding that agencies with existing uses of biometrics (prior to 3 November 2025) will not be required to comply with the Code, and therefore the amended Rule 3A, until after 3 August 2026. Therefore, we believe that Rule 3(A)(1)(10)(b) should state *"before 3 August 2026 in respect of any type of biometric processing by that agency that commenced* ***prior to*** *3 November 2025."*

Notification requirements

The notification requirements may prove operationally heavy, resulting in what may be a significantly increased compliance burden for agencies and the possibility of over-notification for individuals. The requirements for notification under Rule 3A in the BCCP add more requirements than those under IPP3A, and the outcome may be lengthy notifications.

As mentioned in our previous submission on the draft guidance for IPP3A, we have some concerns that there is a risk of “over-notification”, where individuals ignore the notification (via email filters, simply clicking “accept all”, or ignoring the communication all together) and the requirements under Rule 3A fails its intended purpose.

We believe there is tension between ensuring adequate, accessible notification and upholding transparency, and the risk of "black-letter" notification which is technically accurate, yet potentially confusing.

To assist agencies in understanding their notification obligations, we believe more guidance - even using real-world examples of privacy notices - would be beneficial. This is particularly important where the collection of biometric information may be en masse, as in retail environments. Additional guidance would also be beneficial for Rule 3(3)(b), using specific examples to aid understanding on where exceptions for conspicuous notice could apply.

We note the wording of "due particularity", under Rule 3A(1)(b) is more prevalent in the Official Information Act guidance, and suggest that alternative wording may achieve the same intended purpose with more clarity.

Clarity on record keeping expectations and requirements

Agencies without a dedicated Privacy Officer or privacy team will be required to understand and apply a relatively complex piece of legislation with record keeping and external notification requirements, in addition to completing and maintaining multiple risk assessments. The addition of IPP3A, and the addition of Rule 2A extends the compliance burden on agencies, significantly in some cases where a business is complex or relies on multiple flows of data. We believe that additional guidance, in an accessible format, or with frequently encountered situations, may assist agencies in determining how to adjust their frameworks to be compliant and avoid unnecessary complication where possible. For example, it is not clear how agencies indirectly collecting information should be expected to ensure compliance with Rule 3A(1)(2). Expectations of what is "reasonable," if the biometric use is part of a trial period, may vary considerably.

We appreciate there has been guidance already provided for IPP3A, but believe further detailed guidance specifically for the rule changes to each Code could be beneficial for agencies, particularly with examples on which internal record-keeping would be appropriate. For example, should an agency create and maintain a Rule 3A exception register for each type of biometric information indirectly collected, including the specific scenario, exception invoked, supporting evidence as to why, and a review date?

We encourage consideration to the possible steps agencies can take to streamline their compliance and record keeping notifications in light of the operational requirements they may face.

Possible extension of a Privacy Statement

Fonterra suggests that practical compliance and appropriate notification may be achieved via a short privacy notice at the point of collection, which directs to an agency’s complete privacy statement, updated to incorporate the BCCP and IPP3A (for example, on its website). We consider that short privacy notices with clear directions on how more information can be obtained may achieve the intended purpose of the BCCP and Rule 3A. These short privacy notices can supply the information in an accessible format for individuals and reduce the requirements on an agency to supply all information at the point of collection, which may result in numerous forms requiring updating and increasing the risk of multiple notices containing outdated information.

Indirect collection of information where the individual is in a trust, partnership or for AML/ CFT purposes

Agencies subject to the requirements of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 will need to indirectly collect information about people to meet their AML/ CFT obligations. In situations where there is a complex ownership structure, this may involve the collection of information about

directors, shareholders, and individuals in trusts, including collecting documents such as passports which are then submitted for biometric verification.

It may also involve carrying out screening checks (for example, sanctions screening, politically exposed persons screenings) with third-party agencies. These third-party agencies in turn compile data from a variety of sources.

Review of the requirements under Rule 3A suggests that every trustee, beneficial owner, and director whose biometrics are used as part of AML verification processes should receive an individual-level Rule 3A notification. This may be challenging where large, complex structures are in place, and the biometric information is supplied via an authorised business contact. Review of the BCCP and proposed Rule 3A measures suggest that notices provided to the authorised business contact prior to or at the point of collection could satisfy the general exception under IPP3A(3), where an individual has already been made aware of the specific indirect collection. However, further and specific guidance should be provided to give agencies a better understanding on how to effectively meet obligations under circumstances such as those outlined above.

Conclusion

Fonterra supports the intention of the Privacy Amendment Bill, which has the stated aim to bolster transparency on how personal information is collected in New Zealand.

Fonterra believes that compliance with the Bill, as suggested by the draft guidance on IPP3A, is likely to increase the likelihood of individuals receiving multiple communications, leading to notification fatigue as well as placing substantial compliance burden on agencies. This may subvert the intention of IPP3A, and we ask that alternative approaches are considered to meet these obligations such as short privacy notices at the point of collection, which directs to an agency's complete privacy statement.

We would like to see more examples in the guidance outlining how the OPC expects to see agencies comply using a broad range of scenarios, including detailed information about how to apply exceptions. We believe expansion of the guidance will minimise confusion and support counsel and agencies in applying IPP3A appropriately.

Office of the Privacy Commissioner
PO Box 10 094
Wellington 6143

FROM Anchali Anandanayagam
DDI [redacted]
EMAIL [redacted]
MATTER 117936-76
DATE 16 February 2026

By email to IPP3A@privacy.org.nz

Dear Sir/Madam

Consultation on proposed rule 3A – Biometric Processing Privacy Code 2025

Thank you for the opportunity to comment on the information paper regarding the addition of a new rule 3A to the Biometric Processing Privacy Code 2025 (the **BPPC**).

Summary

1. We support the overall intent to incorporate IPP3A into the BPPC but are concerned that rule 3A as interpreted creates inconsistent treatment of biometric versus non-biometric personal information across the same use cases and may be challenging to operationalise in practice. In many deployments, biometric and non-biometric personal information will be captured and processed within the same technology system, meaning agencies will in effect be required to apply rule 3A to non-biometric personal information by default, imposing an unfair compliance burden.

2. The information paper's treatment of the "already been made aware" exception emphasises the need to identify "which agencies" will indirectly collect biometric information but does not clearly carry through the IPP3A guidance's acceptance of category-based descriptions for general notification. The information paper also appears to link the exception to the "clear and conspicuous" standard from rule 3 of the BPPC. Without clarification, this interpretation risks displacing a workable notification regime and fragmenting compliance across biometric and non-biometric information.

3. The proposed wording on "alternatives" to biometric processing is at odds with existing BPPC guidance and risks being read as imposing an additional obligation to affirmatively confirm the absence of alternatives (with little benefit to individuals). We recommend aligning rule 3A commentary with the existing position that agencies need only notify individuals of alternatives that are in fact available.

4. We discuss these issues in more detail below.

Scope of rule 3A

5. We acknowledge that the proposed rule 3A aims to be "consistent" with rule 3 of the BPPC. However, that consistency is itself problematic because rule 3 already reflects a materially narrowed version of IPP3 in the Privacy Act 2020 (the **Act**). The BPPC creates, in effect, a biometrics-only notification regime that is stricter than the general IPP3/IPP3A framework, not merely a tailored implementation of it.

6. We raised these concerns during consultation on the BPPC, including whether it was appropriate for delegated legislation to omit or narrow statutory exceptions in IPP3. Those submissions were not accepted, and rule 3 now stands in a narrowed form. The current proposal takes that narrowed approach as the template for rule 3A, thereby compounding the divergence between the Act and the BPPC.

7. Since the BPPC was issued, Parliament has enacted IPP3A and the Office of the Privacy Commissioner (the **OPC**) has issued detailed guidance on how IPP3A's exceptions are intended to operate in practice, including for sensitive information. IPP3A itself already incorporates Parliament's view on how to balance transparency, practicability and sensitivity: it extends notification to indirect collection but preserves IPP3 exceptions and adds new, targeted exceptions, which can be read alongside the OPC guidance explaining that they are to be applied strictly when used with higher-risk personal information. It is against this changed statutory and regulatory backdrop that the correctness and practicality of further narrowing in rule 3A should be assessed.

Specific comments on proposed exceptions in rule 3A

8. *IPP3A(3) – "already been made aware"*

(a) We support the proposal to recognise IPP3A(3) in rule 3A. However, we are concerned that the information paper unnecessarily restricts the flexible, category-based approach taken in the IPP3A guidance paper in respect of the general notification requirements. We are also unclear how the "clear and conspicuous" standard from rule 3 of the BPPC is now being linked to the "already been made aware" exception.

(b) The OPC's "Guidance on IPP3A" (October 2025) distinguishes between:

(i) The general obligation to tell individuals who the intended recipients of their personal information are; and

(ii) The specific conditions for relying on the IPP3A(3) "already been made aware" exception.

In relation to the first limb, the guidance recognises that agencies may describe recipients using a general description or categories where it is not practical to name every recipient individually. In relation to the second limb, the guidance then requires that an agency relying on the IPP3A(3) exception must itself have been identified to the individual in an earlier notice – that is, the individual must have been made aware that this particular agency may receive their information.

(c) The information paper for rule 3A states that the individual must have "been made aware of the specific indirect collection" and the clear and conspicuous communication "needs to tell the individual which agencies would indirectly collect biometric information to fit within [the rule 3A "already been made aware"] exception". However, under the BPPC, there is no legal connection between the clear and conspicuous communication and the rule 3(3) exception. The "clear and conspicuous" standard is tied to the minimum notification limb of rule 3 under the BPPC, not to every part of that rule. It applies specifically to the basic notice that biometric processing is occurring (and how to get more information), while the remaining rule 3 matters only need to be notified on a reasonable-steps basis, without having to meet the clear and conspicuous threshold.

(d) We are not clear how – as stated in the information paper – the OPC proposes to "align this rule 3A exception with the existing language under rule 3(3)(b)". We assume this means that once an individual has already received a clear and conspicuous notice telling them which agencies will indirectly collect their biometric information, that prior notification can satisfy IPP3A(3), so the indirect-collecting agency does not need to notify again. If that is correct, we recommend the rule 3A commentary specify this clearly.

(e) For the general notification of recipients in IPP3A(1), the IPP3A guidance already permits the use of categories where naming every recipient is not practicable. Without clarification, there is a risk that the biometric-specific language ("which agencies would indirectly collect") could be read as displacing the more flexible, category-based approach to general notification taken in the IPP3A guidance.

(f) We therefore recommend clarifying in rule 3A commentary that agencies may describe categories of indirect collecting agencies to satisfy the general notification requirements under rule 3A. Guidance on rule 3A should also clarify that layered notices (e.g., physical signage plus detailed online privacy information) can together satisfy the "already aware" exception under rule 3A, consistent with the approach already adopted in the IPP3A guidance.

9. *IPP3A(4)(c),(d),(f) – "necessary", "prejudice purpose", "serious threat"*

(a) We support including IPP3A(4)(c),(d) and (f) in rule 3A. These exceptions are particularly important in security and fraud prevention use cases, where notifying an individual that their biometric information has been obtained indirectly could enable them to evade detection or increase risks to others.

(b) It would be useful if the rule 3A commentary repeated and expanded existing OPC guidance examples and explicitly linked them to these exceptions.

10. *IPP3A(4)(g) – research and statistics*

(a) We appreciate the intention to include a research/statistics exception but are concerned to ensure that the proposal to narrow IPP3A(4)(g) by limiting it to situations where information is not "published" does not have unintended consequences. IPP3A itself focuses on whether information will be "used" in a form that identifies the individual, not solely on publication.

(b) In biometric R&D, it is possible to use irreversibly transformed templates, aggregations or other technical controls such that individuals are not identified in the research use, even though the underlying data related to identifiable people. The proposed wording risks excluding such internal research or benchmarking activities from the exception simply because there is a theoretical link back to identifiable individuals, even where strong safeguards prevent re-identification in practice.

(c) We recommend adopting the IPP3A wording (focusing on "use" rather than "publication") and coupling this with biometric-specific guidance requiring de-identification or aggregation, and strict controls on re-identification.

11. *IPP3A(5)-(7) – archiving, security/defence, trade secrets*

(a) We agree that IPP3A(5) (public interest archiving) and IPP3A(6) (security and defence) may be relevant to biometric processing. Given that intelligence and security agencies are excluded from both IPP3A and the BPPC, it would be useful for the OPC to provide illustrative examples so that agencies have practical guidance about using the security and defence exception (e.g., legitimate security related matching in non-intelligence agencies).

(b) We also support recognising IPP3A(7) (trade secrets/prejudice to commercial position) in rule 3A. In complex biometric processing systems, fully explaining every indirect collection pathway may require disclosing vendors, system architectures or proprietary information, which could materially harm commercial interests. We recommend that guidance:

(i) Confirm that high-level or functional descriptions of the biometric processing system and the roles of key participants can be sufficient; and

(ii) Provide examples of when agencies can legitimately avoid disclosing certain technical details while still giving individuals meaningful information.

<u>Overlap and interaction between IPP3A and rule 3A in practice</u>

12. In practice, there may be situations where both IPP3A and rule 3A are relevant, and agencies will have to decide how to comply when the frameworks do not fully align.

13. This could arise, for example, in a commercial scenario involving the use of a multi-party biometric verification system. In this ecosystem, agencies could be subject to the BPPC for their biometric processing activities and to IPP3A for any indirect collection of personal information. Their indirect collection obligations could, therefore, be shaped both by IPP3A and rule 3A:

    (a) IPP3A applies to indirect collection of non-biometric personal information and provides the full set of statutory exceptions, including "not reasonably practicable", "publicly available" and "no prejudice"; and

    (b) Rule 3A, as proposed, would apply to indirect collection of biometric information for biometric processing, but without those exceptions.

14. In that scenario, agencies would therefore have to apply one exception framework to the non-biometric processing components of the verification process (full IPP3A), and apply a different, narrower framework to the biometric processing components (rule 3A), even if both sets of information travel through the same technical pipelines and are presented to individuals in a single privacy notice.

15. This fragmentation makes it harder for agencies to design coherent and comprehensible notification strategies. It would also make it difficult for us to confidently advise agencies on how conflicts between a narrowed rule 3A and the broader IPP3A should be (lawfully) reconciled. In practice, this means agencies will need to unnecessarily comply with the narrower rule 3A in respect of non-biometric processing information. This de facto extension of rule 3A to non-biometric personal information will increase complexity and compliance cost and may deter agencies from adopting privacy enhancing technologies.

16. We recommend that the OPC:

    (a) Treat IPP3A as the primary legal reference point for indirect collection notification (including exceptions); and

    (b) Ensure that rule 3A fully aligns with IPP3A in scope and exceptions, with any biometric processing-specific policies expressed through guidance and enforcement expectations, rather than by further narrowing the BPPC.

<u>Notice of alternatives</u>

17. The information paper states (**emphasis** added):

> We think it makes sense to include the requirement to notify individuals of any alternatives available to them if the agency indirectly collecting their biometric information will conduct biometric processing of that biometric information. This requirement does not mean that an agency needs to provide an alternative. It only requires them to advise the individual **whether or not** there is an alternative available.

18. We are concerned that the last sentence is inconsistent with, or at least misleading when read against, the OPC's existing guidance on the BPPC. That guidance states:

> You only need to tell people about any alternative option that you actually have available to use – not any possible alternative you may have considered as part of your rule 1 assessment.

    The clear BPPC guidance is that where no alternative exists, there is nothing to tell people – agencies are not required to affirmatively state that no alternative is available.

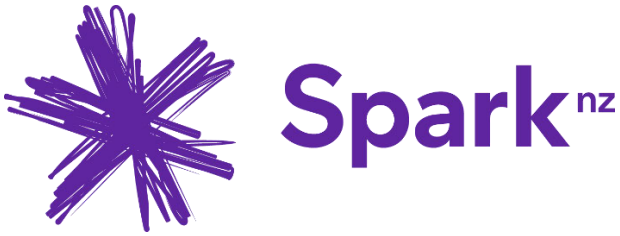
19. The information paper's wording ("advise the individual whether or not there is an alternative available") reads as if agencies must always make a positive statement either way, which either adds an obligation beyond what the current guidance requires or risks being misunderstood as an obligation to positively confirm the absence of alternatives. In either case, there is no practical benefit for individuals. We therefore recommend aligning the rule 3A commentary with the existing BPPC guidance by stating that agencies must inform

individuals of any alternative option that actually exists and is available to them, and clarifying that where no alternative exists, agencies are not required to make a "no alternative" statement (although they may choose to do so as a matter of transparency).

Please do not hesitate to contact us directly to discuss our feedback.

Yours faithfully
Hudson Gavin Martin

Anchali Anandanayagam
Partner



Telecommunications Information Privacy Code IPP3A Consultation

Public Version

Office of the Privacy Commissioner

9 February 2026

Summary

Thank you for the opportunity to comment on the proposed amendments to the Telecommunications Information Privacy Code ("TIPC") to reflect IPP3A.

We are supportive of all of the proposed changes. We also recommend some additional exceptions that we believe will be valuable to

- help ensure clarity on the application of IPP3A to telco specific activities; and
- provide consistency with Rules 2 and 3.

Background

We consider that the TIPC exceptions for collection (Rules 2 and 3) and disclosure (Rules 10 and 11) that specifically relate to the exchange of information between telcos should mirror each other to ensure there is adequate protection for both the disclosing and the receiving party. However currently some of the Rule 10 and 11 exceptions are more comprehensive and broadly drafted than those in Rules 2 and 3. We appreciate that alignment of these exceptions is outside of the scope of this process. However we highlight this inconsistency as

(i) it provides context for the rationale for our aspects of our submission; and

(ii) we believe it's important for any future TIPC changes to maintain consistency with existing Principles where relevant.

Alignment with Rules 2 and 3

With respect to the exceptions for Rule 3A, at a minimum we believe they should fully align with the exceptions set out in Rules 2 and 3. In particular we recommend that in addition to those exceptions already proposed by the OPC, the following Rule 2(2) exceptions are also included as exceptions for Rule 3A.

Rule 2(2)(h): that the information is traffic information;

Rule 2(2)(i): that the collection is an essential element of service provision or the interconnection, wholesaling or similar arrangements between network operators;

Rule 2(2) (j): that the information is necessary to deal with a service or billing enquiry and the collection is from—

(i) a member of the subscriber's household; or

(ii) a representative of a business subscriber;

Alignment with Rules 10 and 11

We consider that ideally the exceptions in Rule 3A would reflect the broader exceptions for collection of data by telcos set out at Rules 10 and 11.

While we note that this proposal does not align directly with the approach set out in section 1.28 of "Information Paper 1 of 5: Proposed Amendments to the Biometric Processing Privacy Code 2025, Credit Reporting Privacy Code 2020, Health Information Privacy Code 2020 and Telecommunications Information Privacy Code 2020" we are noting this as a proposed approach given the current inconsistencies between Rules 2 and 3 and Rules 10 and 11 in the TIPC. For more information on that approach, please see our previous submission dated 24 October 2025.

From: [redacted]
To: IPP3A; [redacted]
Subject: RE: The Privacy Act's IPP3A is here – we need your opinion
Date: Friday, 24 October 2025 11:38:34 am

Kia ora Craig

Thank you for the opportunity to provide feedback on how IPP3A should be applied to the Telecommunications Information Privacy Code 2020 ("the Code"). We believe that the exceptions to IPP3A set out in the Act are appropriate for the Code as they are all potentially relevant in the telecommunications industry. However, as set out below we believe that some of the existing exceptions in the Code specific to the telecommunications industry should also be applicable to IPP3A.

Firstly, regarding interconnection, the nature of telecommunications services necessitates the transmission of personal information between different telecommunications companies' ("telcos") networks. Often, calls are carried across multiple networks to connect callers and enable telcos to provide services. Consequently, telcos constantly receive personal information about individuals with whom they have no direct relationship. The extensive and multi-layered carrier arrangements make it challenging to rely on the individual being aware of the collection of their personal information. While we do not believe that using this information for interconnection services would prejudice the interests of the individual concerned, for clarity, we recommend that the exception currently in use in Rules 10(1)(h) and 11(1)(n) of the Code (see extract below) also be applied to IPP3A.

> *that the [collection] of the information is necessary for—*
> *(i) the provision of a seamless telecommunications service to subscribers; or*
> *(ii) the development or supply of any broadband, intelligent, interactive or multimedia services or other forms of telecommunications service; or*
> *(iii) the provision of a CMS; or*
> *(iv) interconnection, wholesaling or similar arrangements between network operators*

Secondly, with respect to Calling Line Identification Presentation (CLIP), this service inherently involves the collection of personal information from individuals with whom telcos do not have a direct relationship. Again, for the reasons set out above it would be challenging for telcos to rely on the individual being aware of the collection of their personal information. While we do not believe that the collection of this information would prejudice the individual's interests, for clarity, we recommend that the Code's IPP3A Rule also uses the exception currently used in Rule 11(1)(p) of the Code, and excludes the collection of personal information by means of CLIP and in accordance with the requirements of Schedule 3 from the provisions of IPP3A.

Thirdly, subscribers or their representatives will make service and billing enquiries, which necessarily includes information about an individual's communications collected via a third party. Again, while we do not believe that the collection of this information would prejudice the individual's interests, for clarity, logically the exceptions outlined in Rule 11(1)(e) and (m) of the Code are also applicable to the collection of information under IPP3A.

Fourthly, given the critical importance of maintaining the security and integrity of

telecommunications networks and services for customers, we recommend that the exception currently set out in Rule 10(1)(e)(iv) and Rule 11(1)(f)(v) is carried over to IPP3A. This exception acknowledges that non-compliance may be necessary to prevent or investigate actions or threats that may compromise network or service security or integrity.

Finally, concerning complaints about malicious or nuisance telecommunications, Rule 10(1)(g) allows for the use of personal information to investigate complaints and take appropriate action. This sometimes involves calls made from or received by customers of other telcos. We believe it would be helpful if third-party collection of this information was included as an exception to IPP3A. Additionally, it would be beneficial if any future revisions of the Code updated Rule 11 accordingly.

Thank you for considering our feedback. We believe these recommendations will provide clarity and ensure the effective application of IPP3A to the telecommunications industry. We are happy to answer any queries you may have.

Kind regards

Sarah Auva'a
Lead Digital Trust Partner

From: IPP3A <IPP3A@privacy.org.nz>
Sent: Friday, 3 October 2025 8:08 am
To: [redacted]
Subject: The Privacy Act's IPP3A is here – we need your opinion

Tēnā koe

As you may be aware, the Privacy Amendment Act (the Act) has now received Royal Assent. We're emailing you for your opinion on changes this could lead to in the Privacy Act Codes of Practice, which may change how you need to work.

The key change in the Act is the creation of Information Privacy Principle 3A (IPP3A), which will require agencies to let people know when they indirectly collect personal information. IPP3A comes into force on 1 May 2026.

The Privacy Commissioner is considering what changes, if any, may be required to the Telecommunications Information Privacy Code 2020 (the Code).

A round of informal engagement will help us consider whether amendments to the Code are required, and if so, how IPP3A should best be incorporated into the Code.

Your feedback will inform any decision by the Commissioner to amend the Code and what those changes will look like. We will test any potential amendments through formal consultation as required under section 37 of the Privacy Act.

What we want to hear about

We're keen to understand how you think IPP3A should be applied to the Code – in particular:

- Whether the exceptions in the Act are appropriate for the Code, and why;
- Whether you believe there should be fewer exceptions to IPP3A than those in the Act, and why; and
- Whether you believe there should be more exceptions to IPP3A than those in the Act, and why.

Take our survey, or email any feedback to IPP3A@privacy.org.nz by Friday 24 October 2025 so we can start drafting amendments.

The focus of this work is ensuring clarity for the sectors who the Code applies to. Given our resourcing constraints, we are unable to carry out broader amendments to the Code as part of this work.

However, if you have feedback or suggestions for changes to the Code, you're welcome to send this to us for future consideration.

We will be in touch again once formal consultation begins later this year.

Ngā mihi

IPP3A Codes Team

One New Zealand Group Limited

Submission on proposed amendments to the Telecommunications Information Privacy Code 2020

16 February 2026
By email: IPP3A@privacy.org.nz

Introduction

1. One New Zealand Group Limited (One NZ) welcomes the opportunity to comment on the proposed amendments to the Telecommunications Information Privacy Code (TIPC) to reflect the introduction of Information Privacy Principle 3A (IPP 3A) into the Privacy Act 2020, via new TIPC Rule 3A.

2. We support the intent of ensuring individuals are notified when their personal information is collected indirectly. However, we are concerned that the proposed exceptions to Rule 3A do not adequately reflect the operational realities of modern telecommunications networks. Further, if the exceptions to Rule 3A are not sufficiently broad, there is a real risk of "notification fatigue" for telecommunications customers.

3. The OPC's proposed approach appears to focus primarily on alignment with Rule 3. In our view, however, an equally relevant touchpoint is the existing exceptions in Rule 2, given that Rule 2 specifically addresses the indirect collection of information. The Rule 2 exceptions were carefully designed to accommodate the unique characteristics of telecommunications operations, and failing to carry these through to Rule 3A risks creating regulatory gaps that neither protect privacy nor support an efficient and innovative telecommunications sector.

4. In summary, we submit that:

   (a) collection of "traffic information" should be exempt from Rule 3A as it is automatically generated and notification is impractical (see Rule 2(2)(h));

   (b) the exception for collection that is an "essential element of service provision" should be carried through to Rule 3A to support effective service delivery (see Rule 2(2)(i)); and

(c) collection of information from household members or representatives to deal with service or billing enquiries should be exempt – there is no need to provide disclosure in that context, and it creates a compliance burden without any material privacy benefit (see Rule 2(2)(j)).

5. We provide our reasons below.

Collection of "traffic information" should be exempt from Rule 3A as it is automatically generated and notification is impractical (see Rule 2(2)(h))

6. "Traffic information" as defined in the TIPC, is data automatically generated as the result of making a telecommunication. This includes call associated data, such as the originating and destination numbers, time stamps, call duration, and cell site information. By its very nature, traffic information is created as a by-product of network operations, without any active input from the individual concerned.

7. The existing Rule 2(2)(h) exception recognises that it is neither practical nor meaningful to collect traffic information directly from the individual. The same rationale applies with equal force to notification obligations under Rule 3A. Requiring telecommunications agencies to notify individuals each time traffic information is indirectly collected would impose substantial administrative burdens, generate high volumes of notifications with little informational value, and risk contributing to notification fatigue among consumers.

8. Importantly, this exception would not diminish privacy protections. Traffic information remains subject to the TIPC's rules governing storage, security, use, and disclosure. The exception simply acknowledges the operational reality that notification in this context serves no meaningful transparency purpose. We therefore submit that the Rule 2(2)(h) exception for traffic information should be carried through to Rule 3A.

The exception for collection that is an "essential element of service provision" should be carried through to Rule 3A (see Rule 2(2)(i))

9. Rule 2(2)(i) provides an exception where "the collection is an essential element of service provision or the interconnection, wholesaling or similar arrangements between network operators."

10. An equivalent exception should apply under Rule 3A. Delivering telecommunications services to end users requires continuous and seamless information sharing between multiple agencies, including network operators, wholesalers, and service providers.

Much of this information sharing occurs automatically and at scale, often without any direct involvement of the individual subscriber. Requiring notification for each instance of indirect collection in these circumstances would impose significant operational burdens without enhancing transparency or privacy outcomes for consumers.

11. We acknowledge that the proposed Rule 3A(4)(g)(iii) (which we assume should be (4)(i)) includes an exception for "interconnection or the delivery of a CMS". However, this formulation omits the broader language of Rule 2(2)(i) and in our view, should be expanded to include "wholesaling or similar arrangements between network operators" and to include where "collection is an essential element of service provision."

Exemption for information collected from household members / representatives to deal with service and billing enquiries (see Rule 2(2)(j))

12. Rule 2(2)(j) provides an exception where "the information is necessary to deal with a service or billing enquiry and the collection is from (i) a member of the subscriber's household; or (ii) a representative of a business subscriber". This exception reflects the practical reality of how telecommunications agencies interact with customers on a daily basis.

13. When a subscriber contacts their telecommunications provider about a service issue or billing query, it is common for that contact to be made by a household member or, in the case of business accounts, an authorised representative. These individuals typically act with the implicit or explicit authority of the subscriber, and the information collected is used solely to resolve the enquiry for the subscriber's benefit.

14. Requiring telecommunications agencies to notify subscribers each time information is collected from a household member or business representative in this context would generate notifications of no practical value. The subscriber is already aware of the enquiry, has often authorised the contact, and directly benefits from its resolution. Imposing notification obligations in these circumstances would create compliance burdens without delivering any meaningful privacy protection.

One NZ welcomes the opportunity to engage with the OPC on these proposed amendments. We would be happy to discuss any aspect of this submission further or provide additional information that may assist the OPC in its consideration of these matters.

He Kaupare. He Manaaki. He Whakaora.
Prevention. Care. Recovery.

Health Information Privacy Code Rule 3A - ACC feedback

Thank you for the opportunity to offer feedback on the proposed IPP 3A amendments to the relevant codes of practice.

ACC is a health agency, so we have focused our response on the proposed amendments to the Health Information Privacy Code (HIPC). In doing so, we have responded to the questions asked in the HIPC consultation paper, and one of the questions posed in the general information document.

We agree with the proposed approach to incorporating rule 3A into the HIPC. The proposed amendments will clarify ACC's obligations. They should create a more consistent framework for notifying individuals when we collect their health information (whether directly or indirectly).

H1: Do you agree with our proposed approach to exceptions?

Rule 3A:

ACC supports the proposal to retain the exceptions to notification. We do not see issues with the proposed exclusion of the public interest archiving, security and defence, and trade secret exceptions. These are not relevant to ACC's work.

We agree with the proposal to permit notifications to representatives under rule 3A. The proposed approach is consistent with the rest of the HIPC.

Rule 2:

ACC agrees with the proposed amendment to rule 2 (2)(a). However, we note that the proposal creates some inconsistency between rule 2 (2)(a) and (2)(b).

Based on our reading, reliance on (2)(a) would require notification of the matters set out in rule 3A, but reliance on (2)(b) would require notification of the slightly different matters set out in rule 3. Further, where the individual's representative authorises collection from

someone other than the representative themselves, the health agency would effectively be required to notify the representative of both the matters in rule 3 and 3A. That is, rule 2 (2)(b) would require a rule 3 notification, but rule 3A would also apply, given the collection is not from the individual or their representative.

We feel it would be more consistent to amend rule 2 (2)(b) to align with the proposed amendments to (2)(a). However, we recognise that a rule 3 notification is more appropriate than a rule 3A notification when the collection is from the representative themselves (given the collection is essentially direct).

For this reason, we suggest requiring either a 3 or 3A notification, depending on whether the collection is from the representative. This could be achieved by splitting rule 2 (2)(b) into two parts, for example:

> *(b) that the individual is unable to give their authority and-*
>
> > *(i) the health agency collects the information from the individual's representative, having made the representative aware of the matters set out in rule 3(1); or*
> >
> > *(ii) the individual's representative authorises collection from someone else, the health agency having made the representative aware of the matters set out in rule 3A(1).*

H2: Are there tikanga Māori perspectives that we should consider?

ACC assumes we are being asked for a tikanga Māori perspective on the proposed exceptions to indirect notification requirements, rather than a broader response on tikanga perspectives regarding privacy legislation more generally.

The current individual-centric approach under privacy legislation, including the HIPC, is not well positioned to accommodate broader Māori data aspirations. Requiring that whakapapa data be transitioned from a state of tapu to noa, or to provide for Māori data principles, appears to be outside of the scope of the proposed HIPC changes. We do not

see an easy way for the proposed amendments to provide a tikanga-informed approach in information sharing or third-party notification.

From a tikanga Māori perspective, whakapapa data, information about a person's hauora, and the condition of the tinana is seen by many as taonga and tapu. As whakapapa data is connected to whānau, hapū and iwi, it is inherently considered collectively owned. Even if provided in an anonymised fashion, such data still contains mauri. An exception to third-party notification involving whakapapa data impacts more than just the individual. It impacts their whānau, hapu and iwi who have collective ownership interests.

We recognise that the proposed approach to rule 3A (4)(g) is consistent with the current rule 2, which is a practical reflection of an individual's need to share genetic information which may inform treatment outcomes. We further recognise that a requirement to notify family members of collection would create undue complication, as the notification may create administrative and other challenges (particularly in a health context). In addition, the person providing the information may not want any other individual notified for a range of legitimate reasons.

H3: Are there other cultural perspectives that we should consider?

Most Pasifika cultures are collectivist, being that they focus on family, extended family and community rather than the individual. As a result, individuals may consider personal information as something that not only concerns themselves but also impacts and belongs to their family or community. The act of sharing information or providing consent for its disclosure may therefore be regarded as a collective responsibility, rather than solely an individual decision.

Although IPP 3A does not obligate agencies to verify that collective approval has happened before collecting personal information from a third party, the new IPP 3A notification requirements enhance transparency. They should help Pasifika communities better understand how their information is used and shared, empowering them to take any necessary further action.

We have no specific Pasifika perspective or concerns on the exemption for indirect notification where the collection is for the purpose of assembling a family or genetic history.

H4: Do you agree with the proposed approach to drafting, including technical and language changes?

We do not hold any concerns regarding the other changes proposed.

Additional commentary regarding rule 3A guidance:

On the OPC's consultation webpage, we note an intention to develop specific guidance for health agencies handling indirect notifications. We are supportive of the OPC doing this and would welcome the opportunity to participate in this work.

One of the key challenges with implementing IPP 3A (and, if confirmed, rule 3A) is handling mixed personal and health information[1]. ACC regularly collects mixed personal and health information when providing health services to our clients. Enabling rehabilitation and appropriate treatment often necessitates collecting information about the client's wider circumstances. ACC regularly needs to hold information about other individuals in an identifiable manner on a client's claim.

When indirectly collecting mixed personal or health information, IPP/rule 3A starts from a position of notifying each individual involved. However, we are concerned that a 3A notification would inadvertently reveal to individuals that we have collected information about them in relation to another individual's claim. We believe this would negatively impact clients' confidence in ACC's ability to keep their health information confidential.

In the above context, the notification requirement interacts with IPP 6 and HIPC rule 6 in a manner that may confuse the individual(s) concerned. For example, should the non-claimant individual(s) request access to the information referenced in the notification, ACC would likely withhold it to protect claimant privacy. It also introduces a tension with

[1] Mixed personal and health information being information that is 'about' multiple individuals that cannot be neatly distinguished or separated. For example, mental health related documents collected primarily to support the rehabilitation and treatment of an ACC client that contain information about the individuals' relationship with their parents.

IPP 11 and HIPC rule 11, given ACC may not have lawful grounds to disclose information about the claimant to the other individual(s) concerned.

Our position is that exceptions to IPP 3A and rule 3A should generally exempt us from notifying non-claimant individuals about our collection of mixed information. We would appreciate further guidance setting out the OPC's view on how health agencies are expected to handle 3A notifications when they collect mixed information.

G6. Although we are not currently looking at wider amendments to the codes, are there any other comments you want to provide on the codes beyond IPP3A?

There are two areas of the HIPC that ACC believes could benefit from clarification. We appreciate this consultation is intended to focus on Rule 3A, so have attempted to keep our commentary brief. We are happy to provide more information about either area, if OPC would find this useful.

Representative of a deceased individual who has died intestate

ACC is encountering difficulties in dealing with requests for health information about claimants who have died intestate. In many intestacy situations no clear personal representative exists. This can leave ACC without a clear pathway to disclose information in reliance on HIPC rule 11 (a)(ii) or (b)(ii). Requiring family members to seek probate from the High Court is an option, but the cost and delay faced by family members to be granted probate is not efficient.

While there are situations where another exception applies (such as rule 11 (1)(c) or (2)(a)), this is not always the case. This limitation generates operational and fairness challenges for ACC. Release decisions rely on detailed case-by-case analysis, particularly given that the OPC has historically favoured a restrictive approach to disclosure in similar circumstances.

We invite the Commissioner to consider whether the definition of representative is still fit for purpose where it relates to deceased individuals who have died intestate. The Code could be amended to offer, when the deceased individual has no personal representative,

similar flexibility as with persons representing individuals unable to give their consent or authority. In our view this change would be proportionate.

We further note that, unless matching amendments to s 22F of the Health Act were made, Rule 11 (5) wouldn't apply, meaning agencies wouldn't be required to treat such requests as Rule 6 requests. However, a change to the HIPC alone would permit greater flexibility, meaning agencies could consider disclosure of a wider set of information in reliance on (a)(ii) and (b)(ii) on a case-by-case basis.

Loss of health information which has been deliberately disposed of

In *Vivash v ACC* [2020][2], the Human Rights Review Tribunal (HRRT) found ACC had breached IPP 5 because when it destroyed Mr Vivash's physical file, the purpose for which the information had been collected had not been spent. The HRRT found ACC had destroyed the file without considering the progressive degenerative changes being experienced by the claimant and the likelihood that both he and ACC would need to have continued reference to the contents of the file. As such, it concluded that the information was not protected by security safeguards which were reasonable to expect in the circumstances.

ACC holds the view that the HIPC should support the retention of health information where there are genuine clinical benefits to individuals, and where disposal of the information would unreasonably disrupt future clinical benefits to them. Where there is a reasonable belief that the individual won't benefit from prolonged retention, agencies should be able to safely dispose of information, even if there may still be lawful uses for it. Further, the HIPC should be aligned with other legislation regarding the retention of health information (specifically, the Health (Retention of Health Information) Regulations 1996 and Public Records Act 2005).

[2] *Vivash v Accident Compensation Corporation* **[2020] NZHRRT 16**

The OPC could consider amendments to rules 5 and 9 to clarify health agencies' obligations. We acknowledge this topic is complex and would welcome the opportunity to provide further input on it.

Thank you again for the opportunity to comment on HIPC Rule 3A. We are happy to provide further commentary if OPC are to consider broader amendments to the legislation.

Steph Coutts
Manager, Privacy & Ethics & Privacy Officer
ACC

13 February 2026

16 February 2026

IPP3A Codes Team
Office of the Privacy Commissioner
By email: IPP3A@privacy.org.nz

Kia ora koutou

IPP3A and changes to the Health Information Privacy Code

Thank you for the opportunity to submit on the proposed changes to the Health Information Privacy Code 2020 (**HIPC**).

Following the IPP3A changes to the Privacy Act, we are pleased to see those changes now being carefully considered and consulted on in the context of the HIPC, given that the HIPC responds to both the special sensitivity of health information and the unique context in which health services are delivered. Based on the consultation documentation, including the proposed HIPC amendments, we are hopeful that the finalised amendments will:

- recognise the inherent sensitivity of health information
- respond to the unique context in which health services are delivered
- achieve an appropriate level of internal consistency with other rules in the HIPC
- avoid unnecessary complexity or ambiguity, and
- ensure that implementation of indirect collection provisions in the health context is both robust and practicable.

With respect to the last point, we believe it is critical for public confidence that those engaging with the health system are aware how their personal information is treated, but we equally want to ensure that information about this is made available to them in ways which non-intrusively meet their needs. We are particularly concerned that an inflexible or over-prescriptive approach could lead to individuals receiving multiple notifications from multiple agencies as their information travels through parts of the health system, leading to undue concern or irritation at a time when those individuals may already be stressed for health-related reasons.

With these matters in mind, we provide our submissions below.

Health NZ's substantive submissions on the proposed changes to the HIPC

1. Rule 3A(4)

1.1. Submission

With respect to 'prejudice of the interests of the individual concerned' we have considered and acknowledge the commentary in Paper 4 on the recommended approach. However, we submit that there is good reason to retain the Privacy Act formulation in the HIPC, despite the current drafting of Rule 3. The formulation of IPP3A 4(a) – namely that non-compliance would not prejudice the interests of the individual concerned – allows for consideration of other transparency measures which

have been taken by the agency which do not fully meet the requirements of Rule 3A(1) but which do provide the individual with appropriate information on how their information is treated, including avenues for making IPP6 requests of relevant agencies.

We submit that this would allow a flexibility which is beneficial both to individuals and to agencies in implementing IPP3A, while still firmly supporting the principle of transparency with respect to indirect collection. As outlined above, we are particularly concerned about over-notification and complex notifications to individuals as their information travels through parts of the health system, leading to undue concern or irritation at a time when those individuals may already be stressed for health-related reasons. Retaining the Privacy Act formulation would allow for that. This could additionally be supported by guidance to prevent this exception being used in ways which undermine transparency.

Conversely, we submit there is a risk of negative, unintended consequences if the Privacy Act formulation is removed. Agencies may assess full compliance as being impracticable to achieve and rely on the relevant practicability exception. This could potentially lead to *no* transparency measures being in place, undermining the overall intent of Rule 3A. The availability of the non-prejudice exception, with appropriate guidance, would mitigate against this.

We acknowledge this drafting will differ from what is currently provided under HIPC Rule 3, however we believe this is appropriate because the circumstances are different where direct collection is occurring, and where the agency is already interacting with the individual at the point of collection.

While we support retaining the Privacy Act formulation, we also submit that there is value in considering situations where compliance may directly prejudice the interests of the individual concerned. In the context of health information there is a risk that a notification may cause undue distress to a person or risk exposing sensitive details to another person such as a family member. Including an additional clause covering this, preferably supported by guidance, would in our view be beneficial.

Recommendation

We recommend that Rule 3A(4)(a) be amended to follow IPP3(4)(a) as follows:

> *(a) that non-compliance would not prejudice the interests of the individual concerned.*

Additionally, we recommend a new sub-clause under Rule 3A(4) – note the slightly different wording is intended to avoid confusion with the sub-clause above, and is consistent with other HIPC Rules (see, for example, Rule 11(5)(b)(i):

> *(b) that compliance would be contrary to the interests of the individual concerned.*

1.2. Submission

We submit that both Rule 3(4)(c) and Rule 3A(4)(c) should be aligned with the exceptions provided for under Rule 2(2)(h).

Non-compliance for the protection of public revenue is an important exception for Health New Zealand as the largest funder of publicly funded-health services. At times, Health New Zealand will need to recover debt from individuals who have utilised publicly funded health services (usually in hospitals) but are not entitled to claim public funding.

Health New Zealand is not a prosecuting agency, and use of public services when not entitled is not an offence, therefore maintenance of the law would not be applicable in these circumstances. Other exceptions proposed would not enable Health New Zealand to indirectly collect information about individuals for public revenue purposes without notification, which could prejudice the purpose of the indirect collection.

Conduct of proceedings before any court or tribunal is an important exception for Health New Zealand as we may initiate or become involved in proceedings before a court or tribunal which requires indirect collection of information. This exception is likely also necessary for other health agencies including the Health and Disability Commission, health care providers or health authorities responsible for registering health practitioners.

The circumstances above apply equally to Rule 3 – direct collection from an individual as they do to Rule 3A – indirect collection from a third party.

Recommendation

We recommend that the drafting of Rule 2(2)(h) replaces the current drafting of Rule 3(4)(c) and proposed drafting of Rule 3A(4)(d).

1.3. Submission

The example relating to IPP3A where compliance would cause a serious threat to public safety should be reconsidered. Firstly, the example refers to “contagious disease” which it not a term used in the Health Act 1956, the term used should be “infectious disease”. Secondly, it would be more accurate to remove the reference to “the delay caused” and instead refer to “compliance with subrule (1) would cause a serious threat…”. Delay will not be the main reason that compliance with subrule (1) would be difficult, it would likely be urgency and severity of the public health risk, such that it would be difficult to notify individuals of any indirect collection at all. Finally, management of infectious disease, including indirect collection of personal health information is governed under the Health Act 1956 which the example does not acknowledge therefore it places it out of all context. In general, this example about infectious disease would only really apply to Health New Zealand and the Ministry of Health and those actions in relation to infectious disease are governed by the Health Act. Therefore, in practice, this example does not have wide application.

Recommendation

If the Commissioner is minded to retain an example for Subrule 3A(4)(e)(i), we would

welcome engagement to discuss this further.

2. Schedule 1

2.1. Submission on agency (5)

NZ Health Partnerships Limited was a shared services agency owned by the 20 District Health Boards that provided services to the DHBs, including the Health Finance, Procurement and Information Management System (FPIM) and National Procurement services. On 1 July 2022 all of the assets and liabilities of NZ Health Partnerships Limited were transferred to Health New Zealand pursuant to the Health Sector Transfers (District Health Board Shared Services Agencies to Health New Zealand) Order 2022 - 2022/201. NZ Health Partnerships Limited transferred the FPIM assets and liabilities, the national procurement contracts and all other assets and liabilities to Health New Zealand pursuant to the Order in Council. On this basis NZ Health Partnerships Limited no longer handles health information.

Recommendation

We recommend that NZ Health Partnerships Limited is removed from the Specified Health Agencies listed in Schedule 1.

3. Schedule 2

3.1. Submission on agency (13)

Te Aka Whai Ora | Māori Health Authority was disestablished on 30 June 2024 pursuant to the Pae Ora (Disestablishment of Māori Health Authority) Amendment Act 2024.

Recommendation

Accordingly, we support the proposed deletion of the Māori Health Authority from the list of *Agencies Approved to Assign NHI Number.*

Health New Zealand's other submissions on the proposed changes to HIPC

4. Clause 3 – definition of disability support services

4.1. Submission

We submit that the update from "the" to "their" has been omitted.

Recommendation

We recommend that the definition is aligned with the language used in subclause (a) and the definition of disability support services in Pae Ora (Healthy Futures) Act 2022 so that subclause (b) of the definition reads:
…or to the promotion of their inclusion...

5. Rule 3A(3)

5.1. Submission

It is not clear to us why Rule 3A(3) refers to personal information rather than health information. Additionally, the example relating to Rule 3A(4)(e)(i) also refers to personal information when health information may be more appropriate in this context.

Recommendation

We recommend that the references to *personal information* in Rule 3A(3) and Rule 3A(4)(e)(i) are updated to refer to *health information*.

6. Other feedback on the HIPC

6.1. Submission Rule 4(1)(b)

Rule 4(1)(b) refers to *personal information*, not *health information* or *information*.

Recommendation

We recommend that Rule 4(1)(b) is updated to refer to *health information*.

6.2. Submission Rule 6

Rule 6 is titled *Access to personal health information*, rather than *Access to health information.*

Recommendation

We recommend that the word *personal* is deleted from the Rule 6 heading and that a consequential amendment is made to the index to the HIPC.

6.3. Submission Rule 13

There are a number of roles that are registered with a professional body but do not fall within the strict definition of the health practitioner in the HIPC that are common in the health sector. By way of example, the following healthcare professions have professional bodies but are not regulated under the Health Practitioners Competence Assurance Act:

- Speech language therapists
- Audiologists
- Counsellors
- Pharmacy Technicians and Pharmacy Accuracy Checking Technicians
- Hearing therapists
- Alcohol, other Drug, and Problem Gambling Practitioners, and
- Social Workers.

The definition of health practitioner in the HIPC limits the workforce which can be identified using the CPN. This in turn, has an impact on Health NZ systems which require identification of an individual providing health services, for invoicing, referral, discharge planning, and other tasks as delegated to or enabled by those roles.

Recommendation

We recommend that the following new definitions are added to clause 3(1):

> **healthcare worker** means an individual qualified, or in training to be qualified to provide health services (whether paid or unpaid) and is registered with a professional body that is not a health professional body.
>
> **professional body** means a body responsible for the registration of healthcare workers that are not health practitioners.

As a consequential amendment, we recommend that *healthcare worker* is added to:

- Clause 4(2)(d) after the word *health practitioner*
- Rule 11(2)(b) after the word *health practitioner*
- Rule 11(2)(k) after the word *health practitioner, and*
- Rule 13(4) after the word *health practitioner.*

As a further consequential amendment, we recommend that *professional body* is added to:

- Clause 4(2)(f) after the word *health professional body, and*
- Rule 13(4)(a) after the word *health professional body*.

We are available to engage with you in more detail on this submission.

Guidance for indirect notification under HIPC

We welcome the opportunity to make submissions on the guidance for indirect notification requirements under the HIPC as part of your consultation process later this year.

In particular we would welcome further guidance on the interactions between Rule 2(2) and Rules 3 and 3A.

Further information

Health New Zealand also welcomes any further opportunity to provide more detailed feedback on the proposed changes to the HIPC. We would be pleased to answer any of your questions or meet with you to discuss our recommendations.

Ngā mihi

Viv Kerr

Head of Privacy

16 February 2026

Craig McWilliams
Senior Policy Advisor
Office of the Privacy Commissioner | Te Mana Mātāpono Matatapu
PO Box 10094
WELLINGTON 6011

By email: [redacted]

Tēnā koe Craig

Office of the Privacy Commission - Draft Guidance on the Privacy Code of Practices – incorporating Privacy Principle 3A

Introduction

The Royal New Zealand College of General Practitioners (the College) welcomes the opportunity to comment on the draft guidance issued by the Office of the Privacy Commissioner concerning amendments to sector codes, including the Health Information Privacy Code, and the introduction of a new Rule 3A (IPP3A) to align with the Act and code-specific exceptions. IPP3A, introduced through the Privacy Amendment Act 2025, takes effect on 1 May 2026.

The College submission specifically comments on the introduction of new obligations and the impact on general practices, as the new requirement specifies, agencies that collect personal information from sources other than the individual must take reasonable steps to notify patients when information is collected indirectly, unless an exception applies.

Across Aotearoa New Zealand, specialist GPs and clinical teams manage 24 million patient contacts each year, generating approximately 15 million patient test results a week. This vast volume of clinical information supports safe and coordinated clinical care. Mandating item-by-item notification to patients for all indirectly collected, non-productive health information is not possible or feasible without displacing clinical time.
It would create significant administrative burden, delay care, and introduce safety and equity risks, given the extraordinary volumes of routine, clinically expected information received by practices each day.

- The new rule would require specialist GPs to notify patients about every item of indirectly collected information and explain why.
- Attempting to meet the IPP3A new rule requiring indirect notification for every patient test result would significantly increase demands on clinical time, create bottlenecks, and delay patient care.
- The operational reality of requiring indirect notification for every patient, as an item-by-item notification duty is not feasible due to the volume of routine inflows such as lab results, discharge letters, and specialist correspondence arriving in extremely high volumes, e.g., results, discharge letters, specialist correspondence.

Our position

The College upholds patient information rights; however general-notification of indirect information is considered best practice; it is safer, more equitable, and avoids flooding patients with routine or duplicative messages. It preserves scarce clinical time and supports equity for patients who do not have access to patient portals. This approach ensures focused engagement when it matters for care, while also meeting the transparency intent of IPP3A.

Office of the Privacy Commissioner Questions

1. **What are GPs currently thinking about this obligation?**
   The College supports greater transparency and patient information rights, but the application of IPP3A as an item-by-item notification duty for all indirectly collected health information is not feasible in general practice settings. In general practice,

   Currently, 56 % of GP time is spent on patient consultations and 31% on non-contact clinical work. Our research to understand how specialist GP time is spent shows the significant volume of non-contact clinical tasks already required by specialist GPs and clinical teams. [i] Given the current scale of indirect information flowing into practices, additional work that reduces consultation time for patients would significantly undermine the ability to provide safe, consistent continuity of care.

2. **Have you received requests for assistance from GPs?**
   Most specialist GPs are not currently focused on the implications of IPP3A, given the number of competing access and system pressures such as patient wait times such as, increases in patient populations, increase in health needs related to inequity, people with complex and higher health needs, and the Manage My Health portal safety concerns.

   The RNZCGP Quality Programme supports approximately 1077 general practice teams to understand their obligations with meeting privacy requirements. At present, GPs only notify patients when incoming information is clinically significant, requires action, or needs discussion. Routine correspondence is filed in the patient record without direct notification. While some patients may receive automated alerts through portals when information is filed, many patients are not enrolled in portals, meaning current notification pathways are inconsistent across the sector - this is an equity issue.

3. **What are some common examples of indirect collections that you think should be reflected in the guidance?**
   Indirect collections cover all routine, high-volume inflows to practices (e.g., tests and lab results, discharge letters, specialist correspondence. The list below is an example of the range of tests and results that come into general practice practice every day:
   - Lab results – where the tests have been ordered by the provider.
   - Lab results – which the GP has been ‘copied in’ to, from another provider.
   - Radiology results – again, some ordered by the practice, but many where the GP has been “copied in” by ED or another provider.
   - Discharge letters – from hospital /ED /allied health providers.
   - Outpatient/Specialist letters – in some cases where the GP has referred, but quite commonly where the appointment has been requested by the hospital or someone else – so not specifically requested by the GP.
   - Crisis team letters – where crisis team has been called out to see patients in acute mental health crisis.
   - After hours clinic letters – where a patient has seen an after-hours or telehealth provider.
   - Letters from police (e.g., firearms licences), from Oranga Tamariki (usually asking for information but often providing some information as well).
   - Letters from screening programmes – sometimes with results or raising concerns about non-attendance.

- Letters from worried relatives and neighbours – sometimes specifically asking that the letter is not shared with the patient.
- Letters from insurance companies and ACC often request information but sometimes share it.

4. **What do you think the main concerns/difficulties about complying with this obligation will be?**
The main challenge for general practice clinical teams is the sheer volume of indirect information GPs receive—much of which patients are not aware is coming into their record, such as results copied from other providers or screening programme correspondence. Covering routine inflows from labs, radiology, and other providers within an updated privacy statement would therefore be highly beneficial. While portal notifications can help, many patients are not enrolled in portals, and given recent negative publicity uptake may decline further.

   Clear guidance is also needed on how to manage information received from agencies that are not directly involved in a patient's care, such as Oranga Tamariki, Police, ACC, insurers, or concerned family members. The more that can be addressed through the privacy statement, the more workable compliance will be for general practice.

   We recommend that proposed guidance for indirect notification of by the Office of the Privacy Commissioner (OPC) implements IPP3A in health via general notifications through updated privacy statements, and notices, this is consistent with how IPP3 is commonly met, and would be supplemented by practical, sector-specific guidance for common health scenarios and clear application of exceptions.

Thank you for the opportunity to meet with your team during the early consultation phase. Our submission clarifies the points we raised.

Nāku noa, nā

Dr Prabani Wood
BA, BMBCh, MPH, FRNZCGP
Medical Director | Mātanga Hauora

[i] Bradford L, Wright S, Schulde J, Murton S. The seen and unseen work of general practice: a national diary study of New Zealand General Practitioners. 23 January 2026. *J Prim Health Care* HC25195. Available at: https://doi.org/10.1071/HC25195

Te Kaunihera Rata o Aotearoa | Medical Council of New Zealand

PO Box 10509
Wellington 6140
New Zealand

+64 4 384 7635
0800 286 801
mcnz@mcnz.org.nz
mcnz.org.nz

23 February 2026

Mr Michael Webster
Office of the Privacy Commissioner
By email: IPP3A@privacy.org.nz

Tēnā koe Mr Webster

IPP3A implementation and the Health Information Privacy Code 2020

1. Thank you for the opportunity to provide feedback to your consultation on proposed amendments to the Health Information Privacy Code 2000 (HIPC) and how Information Privacy Principle 3 A (IPP3A) can be accommodated within the code.

2. This paper sets out Te Kaunihera Rata o Aotearoa I the Medical Council of New Zealand's (the **Council's**) feedback on the proposed guidance and our concerns regarding the application of Information Privacy Principle 3A (**IPP3A**) to those in our circumstances.

Background

3. The Council is a statutory body that regulates New Zealand medical practitioners. The Health Practitioners Competence Assurance Act 2003 (**HPCAA**) sets out the Council's role which includes: registering doctors, setting standards for the way doctors practise medicine, making sure doctors have the skills to practice within their scope of practise, and reviewing doctors when their performance, professional conduct, or health is a concern. The Council is not deemed a public sector agency.

4. To carry out its functions under the HPCAA, the Council (and its agents) frequently collect or receive personal information about individuals from sources other than the individual concerned.[1] In some circumstances, the individual concerned is unaware that the Council and/or its agents hold their personal information.

[1] An agent of the Council is a person who is employed on a fixed term, contracted, casual or ad hoc basis to undertake a specified role/ task and/or perform a statutory function, but acts independently of the Council. This may include (but is not limited to): a vocational practice assessor, an educational programme supervisor, a health case assessor, a performance assessment committee member. a professional conduct committee member, a preliminary competence inquiry assessor or reviewer, an examiner, actor or other contractor for the NZREX Clinical examination, a prevocational educational

Submission

5. The Council makes the following points:
    a) The Council wholeheartedly agrees with your Office's approach to data minimalisation. We also agree that personal information should only collected, used and disclosed in the manner set out in the information privacy principles in Privacy Act 2020.
    b) The Council supports guidance for organisations, and in particular for organisations in the health sector.
    c) As a regulator, the Council is not a public sector agency and does not fit neatly into the 'maintenance of the law' exceptions provided in IPP3A. We will need to rely on other exceptions to maintain our current notifications processes and to reduce the need to allocate resources solely to meet the requirements of the Act.
    d) The Council is willing to employ a multi-pronged strategy to meet the requirements of the amendment and the proposed guidance under the Health Information Privacy Code. We would like to balance this with robust and accessible guidance so that we can progress with confidence.

Useful Guidance

6. Council would like to specific guidance in the following situations:

    a) For regulatory authorities (RAs) under the HPCAA broadly, where they can adhere to IPP3A while also upholding the privacy and natural justice obligations to the health professional under investigation and its obligations under the HPCAA to "protect the health and safety of members of the public".

    b) For organisations relying on exceptions, clearer examples that are specifically illustrating what is 'not practicable' in the circumstances. For example, when dealing with large volumes of personal information on a regular basis.

    c) When the onus lies on the Council to disclose information, in the light of the rights of natural justice that are owed to all parties, when should disclosure take place?

    For example, a doctor's notification is confidential to Council, the doctor, the notifier (who is not always the patient) and their representatives until a conclusion is reached. This may be within:

    - 3-4 months at our triage team stage, or

supervisor, or an accreditation panel member. Under the Privacy Act, we understand that it may also include entities that holds information on our behalf e.g., software vendors/ recruitment agencies/marketing agencies.

- up to 4-6 months to Council,
- up to a year at a Professional Conduct Committee (PCC), or
- 1-2 years at a Health Practitioners Disciplinary Tribunal hearing.

We can foresee a situation where a patient or their family will be distressed to learn we used this information for the investigation and prosecution for years before letting them know. On the other hand, to disclose it earlier would be to prejudice the rights of the doctor, or risk making the proceedings public.

d) If the Council or a Council agent collects personal information from Organisation A, who collected it from Organisation B, what organisation holds responsibility for informing the individual concerned about the collection? For example, if a PCC collects the investigation file from the HDC, which includes patient records the HDC obtained from a GP clinic – who is responsible for informing the patient concerned about the collection?[2]

e) The Council seeks further clarification on the point at which an organisation or its agent with investigatory powers could use the exception "non-compliance is necessary for the conduct of proceedings before any court of tribunal (being proceedings that have been commenced or are reasonably in contemplation)". This addresses the possibility that any notification regarding a doctor's conduct may be referred to the HPDT.

f) We seek further information on the application of the exception that "compliance would prejudice the purposes of the collection" in the context of regulatory investigations.

g) We seek the OPC's view on how section 11 of the Privacy Act applies to Council agents that are appointed by the Council to perform a statutory function, but act independently of Council and uses information for its own purposes.

No prejudice to the individual – IPP3A(4)(a)

h) Under the Privacy Act, IPP3A(4)(a) creates an exception where *non-compliance would not prejudice the interests of the individual concerned*. The proposed HIPC equivalent sets a higher threshold: *compliance would prejudice the individual's interests*.

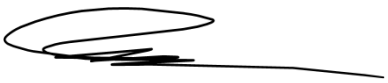
i) While we understand the desire to align exceptions across related HIPC rules

[2] This relates to our obligations under paragraph (3) of IPP 3A.

(e.g. rules 3 and 3A will have similar thresholds), the two rules operate in different contexts. HIPC rule 3 governs a narrower and more proximate situation — collecting information directly from the individual — whereas the new rule 3A is more likely to apply to larger collections of information. The exception will have less utility in these scenarios. For example, the Medical Council (or its agents) routinely collects substantial prescription data when assessing notifications about doctors' prescribing practices. Under the Privacy Act, the existing exception may legitimately apply to many of these individuals. However, because this is health information, the HIPC applies instead, and the proposed amended exception does not clearly accommodate such situations. From a policy perspective, if an individual is not informed of an indirect collection of their information but this causes them no prejudice (and is of course otherwise lawful), then their interests are protected. While we understand that other exceptions may apply (e.g. that 'compliance is not reasonably practicable in the circumstances' – IPP3A(4)(e)), having a more specific exception would assist agencies when navigating their compliance obligations.

The Council looks forward to working with your Office on this guidance, we would be pleased to be involved in providing whatever assistance is required.

Nā te Kaunihera



Kiri Rikihana
Manukura Tuarua
Deputy CEO and Privacy Officer

WOTTON KEARNEY

23 February 2026

Office of the Privacy Commissioner
IPP3A Codes Team

By email IPP3A@privacy.org.nz

IMPLEMENTING IPP3A INTO HEALTH INFORMATION PRIVACY CODE — MPS SUBMISSION

1. We act for the Medical Protection Society (**MPS**). MPS is the professional indemnifier for over 85% of medical practitioners in New Zealand. This cohort is, collectively, a significant stakeholder in the health information privacy space.

2. The Privacy Amendment Act 2025 (**Amendment Act**) has introduced a new information privacy principle (**IPP**) 3A — which will come into force on 1 May 2026. The Privacy Commissioner has proposed amendments to the Health Information Privacy Code (**HIPC**) to implement IPP3A and has invited submissions in respect of the same.

3. The HIPC has the same force and legal standing as the IPPs in privacy legislation,[1] and within it, the requirements of IPP3A can be modified to address the unique and specific needs of the health sector.[2] MPS seeks to ensure IPP3A, once implemented, is workable and does not unnecessarily inhibit the efficient provision of good quality healthcare.

Relevant context

4. IPP3A will require agencies to notify individuals when they indirectly collect those individuals' personal information. The stated intent behind this is to enhance 'transparency and control' over information that is not collected directly from the individual concerned.

5. It is submitted that maintaining transparency in respect of each and every instance of collection of health information (distinct from the *use* or further *disclosure* of that information — which are already subject to clear limits[3]) would not necessarily be welcome or required privacy enhancements for individuals in the healthcare context.

    5.1 By its nature, the collection and compilation of health information is ongoing and interrelated. Information collected as part of one episode of care is often required by or useful to other health providers in the future.[4] Indirect collection of health information is, accordingly, exceptionally common, particularly for general practitioners (**GPs**). Examples of regular and/or expected instances of indirect collection are set out in *Appendix A*.

    5.2 Most health information is collected in the context of a health professional/patient relationship (in a situation of confidence and trust), with an awareness — or indeed, an expectation — that information may be indirectly exchanged to facilitate the improvement and/or maintenance of the patient's health.

[1] See: Privacy Act 2020, s 38 and *Urlich v Police* [2019] NZHC 457 at [20].
[2] *Te Pou Matakana Ltd v Attorney-General* [2022] 2 NZLR 148 at [32].
[3] HIPC rules 10 and 11.
[4] *Te Pou Matakana Ltd v Attorney-General* [2022] 2 NZLR 148 at [33].

Level 12, 342 Lambton Quay
Wellington 6011, New Zealand | Aotearoa
PO Box 5530, Wellington 6140, New Zealand | Aotearoa

WOTTON KEARNEY | **WELLINGTON | TE WHANGANUI-A-TARA**
E: newzealand@wottonkearney.com **W:** www.wottonkearney.com
T: + 64 (0) 4 499 5589

6. In these circumstances, it is submitted there will often be no enhancement of trust or substantive benefit on a patient's part in being notified that certain information has been received, where nothing further is proposed to be done with that information, at that point.

7. The Privacy Commissioner recognises privacy rules for the healthcare sector need to support timely and effective care for individuals who require health services.[5] The context of the sector is relevant and must be considered in imposing further regulatory requirements. The healthcare system in New Zealand is overburdened and under-resourced — and this is particularly the case for primary care. Compliance expectations imposed must be proportionate to the privacy interests at stake. If requirements are too onerous, the inevitable result is they may simply not be able to be achieved (at least not without diverting resources and eroding the quality of care). This will layer more pressure on a workforce already facing high levels of burnout. And it may disincentivise the practice of providers (particularly GPs) proactively, indirectly collecting information in respect of patients — to ensure a complete understanding of a patient's situation. Electing not to do so would degrade the quality of care. It could also put GPs at risk of not meeting professional and ethical obligations, or the expectations of medical regulators, to provide properly informed and coordinated care.

8. To be workable and effective, the HIPC must enable accessible pre-emptive compliance with IPP3A notification requirements, and clear and accessible exceptions to notification requirements, where appropriate.

Pre-emptive compliance

HIPC rule 2

9. Generally, if a health agency collects health information, the information must be collected from the individual concerned (rule 2(1)). An agency can only collect health information from someone other than the individual if an exception in rule 2(2) applies.

2(2)(d)

10. Where an individual's health information is collected from a third party, without notice and unbidden (a common occurrence, particularly for GPs), it is submitted the rule 2(2)(d) exception should apply. This would make sense; direct collection of the health information from the individual concerned would not be 'reasonably practicable' or required, when an agency already has it.

11. With the 2(2)(d) exception made out, the privacy protections in the proposed rule 3A would then apply. The proposed rule 3A(2) confirms the prescribed notification can take place after health information has been indirectly collected.

12. It is submitted the indicated health-sector guidance that will be published in respect of IPP3A should confirm rule 2(2)(d) can be applied in this way.

HIPC rule 3A

3A(1)

13. The proposed rule 3A(2) confirms that notification of the matters in 3A(1) can occur *before* or *after* health information is indirectly collected. The proposed wording in 3A(1) should be amended to make clear that both options are available.

14. 3A(1)(d) proposes to require notification of:

> *…(d) the name and address of—*
> *(i) the health agency that has collected the information; and*
> *(ii) the health agency that is holding the information…*

[5] Privacy Commissioner *Information Paper 4 – Adding rule 3A to the Health Information Privacy Code 2020* <20260108-IPP3A-HIPC-Information-Paper-A1150470.pdf> (**Information Paper 4**).

15. Structuring (d) as above, could be interpreted to require the specification (name and address) of two agencies: the one that has indirectly collected health information and the one that holds it.

16. Where rule 3A(1) can apply before health information is indirectly collected, it is submitted there is scope to interpret 'the health agency that is holding the information' as the agency from which the information will be received/collected. A perception that the 'name' and 'address' of the *provider* of the information must be notified would, in many situations, make pre-emptive satisfaction of 3A(1) impossible. Health providers regularly receive information from various unknown providers, and they could not specifically identify who those providers are or may be, in advance.

17. The Privacy Commissioner's 'Guidance on IPP3A' (**2025 Guidance**) explains the intended application of 3A(1)(d). It clarifies "*for the purposes of IPP3A, the 'agency that holds the information' is considered to be the agency collecting the information indirectly.*"[6] This would be more clearly reflected in (d) by removing the separated sub-particulars (i) and (ii) — and describing the specification requirement as applying singularly to the agency that collected and thus holds the relevant information.

18. The proposed changes can be implemented in the HIPC as follows:

Rule 3A
Collection of health information other than from individual concerned

(1) *If a health agency collects health information about an individual other than from the individual concerned or from the individual's representative, the health agency must take any steps that are, in the circumstances, reasonable to ensure that the individual concerned, or their representative, is aware of—*

(a) *the fact that the information is being or has been collected; and*

(b) *the purpose for which the information is being or has been collected; and*

(c) *the intended recipients of the information; and*

(d) *the name and address of ~~(i)~~ the health agency that is collecting or has collected, and is holding or will hold the information; and ~~(ii) the health agency that is holding the information; and~~*

(e) *if the collection of the health information is authorised or required by or under the law, the particular law by or under which the collection of the information is authorised or required; and*

(f) *the rights of access to, and correction of, health information provided by rules 6 and 7.*

Fact of collection

19. Addressing 3A(1)(a), the 2025 Guidance confirms it will be permissible to identify 'the kind of information' collected. This is appropriately broad. Identification of the specific/particular information in issue in every instance of indirect collection would not be workable in the healthcare context. It would render instances of necessary, pre-emptive notification of collection impossible.

20. The ability to notify patients of instances of indirect collection in general terms — for example, that 'hospital discharge and/or specialist letters' will be indirectly collected from other health providers, to ensure an understanding of the patient's condition and care received — must be enabled.

Intended recipients

21. Addressing 3A(1)(c), the explanatory note in the 2025 Guidance states health agencies should "*tell people who you will be sharing their information with*."[7] The Guidance contains an example of sharing

[6] Privacy Commissioner *Guidance on IPP3A – Notification requirements for indirect collection of personal information* October 2025 <20251216-IPP3A-guidance-finalised-for-web-A1135067.pdf> (**2025 Guidance**) at 10.
[7] 2025 Guidance at 9.

collected information with 'a particular agency'. In this circumstance, we would expect rule 11 of the HIPC (addressing disclosure) would apply.

22. It is submitted it would be more appropriately targeted to IPP3A if the intention of this notification of 'intended recipients' requirement was to enable an understanding of who might *access* information indirectly collected and held.

23. For workability, in the healthcare context, general descriptions of intended recipients (type/class/category) must be permitted. For example, if a discharge summary is indirectly collected, recipients who may access it could include: 'the patient's GP, and any other doctors or nurses at [practice name] who have a clinical justification to access the information'.

3A(2)

24. 3A(2) addresses when notification of 3A(1) matters can occur.

25. The 2025 Guidance appropriately recognises that technical and resource considerations may influence what is a 'reasonably practicable' timeframe for notification.[8]

26. The 'Sterling Draper' marketing list example in the Guidance also proposes a delay in notifying of an indirect collection of information may be justified, where more effective and fulsome notification could occur within a planned future communication.

27. Enabling a practice like this would be beneficial — for efficiency, and effectiveness — in the over-burdened healthcare context. It is appreciated the collecting health agency would need to justify the timing, but acknowledging acceptance of a degree of flexibility is important.

3A(3)

28. The proposed 3A(3) confirms the 3A(1) notification requirements can be fulfilled pre-emptively.

29. The acknowledged broad way notification can occur ("*by any means*") is appropriate where information in a healthcare context is imparted to patients in various ways, i.e. directly in discussion; via practice policies, privacy statements, contracts; or through notification in online patient portals. The 2025 Guidance develops this further through acknowledging the option of 'layered' notification — enabling, for example, brief privacy notices on forms or signs, supplemented by longer notices made available online or in brochures.[9] This flexibility to impart the 3A(1) information is likewise suitable and necessary. Factors to work around include immense time pressures and ensuring appropriate and effective communication, having regard to the particular patient in question.

30. The 2025 Guidance addresses an option of a disclosing agency fulfilling the 3A(1) notification requirements on a collecting agency's behalf.[10] Utilising 3A(3) in this way has limited practical benefit or relevance in a healthcare context:

    30.1 There are rarely enforceable contractual arrangements between health agencies that share health information about patients (i.e. Te Whatu Ora (hospitals)/GPs; GPs/specialist providers) through which notification expectations could be enforced.

    30.2 There may be little incentive on a disclosing agency's part to take on fulfilling another agency's obligations, as well as their own, when they may operate in the same pressurised and under-resourced context. This is particularly so where the specificity requirements (i.e. the 'name' and 'address' of the collecting agency) would in many cases prohibit general notification practices. The disclosing agency would not meet requirements by saying "*we will provide health information collected to 'your GP'*". That GP's 'name' and 'address' is required.

[8] 2025 Guidance at 8.
[9] 2025 Guidance at 6.
[10] 2025 Guidance at 19-20.

30.3 To be certain and assured notification met requirements, providers who collect the information would need to 'check' the actions of the disclosing agency — and in doing so may create an even greater workload, than achieving the notification requirements themselves.

31. Addressing the proposed provision, the minor change in 3A(3) below should be made, for consistency with the rest of 3A — which refers to 'health information':

> *(3) A health agency is not required to take the steps referred to in subrule (1) in relation to the collection of ~~personal~~ health information if the individual concerned, or the individual's representative, has previously been made aware by any means of all of the matters specified in subrule (1) in relation to the health agency's collection of the information.*

Exceptions to notification requirements

4(a) – prejudice interests

32. The 3A(4)(a) exception is proposed to be implemented into the HIPC in a different way than it is included in the Amendment Act.

32.1 The exception to notification in the Amendment Act is accessible where: non-compliance would not prejudice the interests of the individual.

32.2 The proposed exception in the HIPC proposes: notification is not necessary if compliance would prejudice the interests of the individual concerned.

33. The higher threshold proposed in the HIPC is not necessary or justified — where the regular, necessary, and oftentimes known and accepted practice of the indirect exchange of health information between providers is considered.[11] The entrenched practice exists to benefit patients, and it is submitted being notified of indirect collection would be an unwanted intrusion in many circumstances.

34. The aims and ends of the indirect collection of health information differ from justifications underlying the collection of information directly from a patient. Direct collection may occur where the information sought is more material, prompting an enhanced interest on a patient's part in knowing what will be done with it/how it will be treated.

35. The stated rationale for aligning 3A(4)(a) with 3(4)(a)(i) of the HIPC (and not the Amendment Act) is premised on the nature of the information in question, being health information.[12] It is submitted this is too narrower focus. The circumstances of it being collected should be a relevant consideration.

36. Incorporating the 4(a) exception on the same terms as it exists in the Amendment Act retains the protection offered by the 'reasonable belief' qualifier/condition. An agency must be confident and able to justify that not notifying of the 3A(1) matters would not prejudice the interests of the individual concerned. If it was considered not knowing would cause prejudice, the exception could not apply.

37. It is submitted 3A(4)(a) should be implemented in the HIPC as follows:

> *(4) It is not necessary for a health agency to comply with subrule (1) if the health agency believes, on reasonable grounds,—*
>
> > *(a) that non-compliance would not prejudice the interests of the individual concerned;…*

[11] Addressed at paragraph [5] above.
[12] Information Paper 4 at 4.

4(c) – not reasonably practicable

38. The 2025 Guidance identifies that if the information in question is sensitive, then the threshold of 'not reasonably practicable' will be higher.[13]

39. While health information by its nature is sensitive and attributed high privacy value, as addressed above, the circumstances of it being indirectly collected might be of little interest or significance to a patient.[14]

40. The circumstances/context of collection should be a factor to consider in assessing whether the efforts undertaken to notify were sufficient (as opposed to the nature/type of the information alone). This is particularly important in the healthcare context, where there is broad understanding that the sharing of health information between providers is regular and necessary to facilitate continuity of appropriately targeted care.

Concluding comments

41. We and MPS are happy to meet to discuss this submission, or to provide further information.

42. MPS notes, with appreciation, the Privacy Commissioner's intention to produce specific guidance on IPP3A for the healthcare sector. It is submitted this should contain practical examples of how the requirements can be achieved in practice. The MPS is eager to be consulted in respect of this guidance.

Yours sincerely

Kate Wills
Senior Associate
D: [redacted]
E: [redacted]

Adam Holloway
Partner
D: [redacted]
E: [redacted]

[13] 2025 Guidance at 24.
[14] For example, where a person's GP is copied into a letter notifying of a hospital discharge, with no further action from the GP required.

APPENDIX A

Regular and/or expected instances of indirect collection of health information

- Receipt of laboratory, radiology or other results ordered by a provider.
- GPs being ‘copied into’ laboratory, radiology or other results ordered by another provider (providers are encouraged by medical regulators (i.e. the Health and Disability Commissioner) to send copies of information to GPs, to ensure informed continuity of care).
- Consulting platforms such as ‘HealthOne’ to check a patient’s medical history and current prescribing (as expected by medical regulators).
- Receipt of discharge, outpatient or specialist letters, from hospital/ED/after-hours providers/allied health providers/secondary providers (including GPs being ‘copied into’ the same).
- Calling the hospital to seek advice about a patient’s presentation, where the hospital may then convey information gleaned from the hospital’s records.
- Calling the hospital to enquire after a patient referred there for further investigation (to check if they have accessed required care).
- Receipt of Mental Health Crisis Team letters, where the Crisis Team has been called out to see a patient experiencing an acute mental health event.
- Receipt of letters from screening programmes, with results, or raising concern about non-attendance.
- Contact from Police, Oranga Tamariki, insurance companies, the ACC.
- Receipt of letters from employers, regarding, for example, fitness to work.
- Unsolicited contact from concerned relatives or neighbours, sometimes with a request that a patient not be informed of the contact.

24 February 2026

Office of the Privacy Commissioner
IPP3A Codes Team

By email IPP3A@privacy.org.nz

IMPLEMENTING IPP3A INTO HEALTH INFORMATION PRIVACY CODE — MEDICAL PROTECTION SOCIETY — ORGANISATIONAL IMPACT

1. We act for the Medical Protection Society (**MPS**). The MPS has — separately — made a submission to the Privacy Commissioner on the proposed implementation of IPP3A into the Health Information Privacy Code 2020 (**HIPC**), advocating for the interests of its members.[1]

2. This submission addresses:

   2.1 the implications of the proposed implementation of IPP3A into the HIPC for MPS, as a professional indemnity organisation; and

   2.2 a submitted appropriate response, namely:

      (a) the expansion of the proposed 3A(4)(d) 'maintenance of the law' exception to allow for non-compliance with 3A(1) notification requirements, where believed reasonably necessary:

         (i) to avoid prejudice to the maintenance of the law where information is collected by an indemnifier or adviser for the purposes of claims management services and/or advice and/or legal advice to healthcare providers; and

         (ii) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); and

      (b) confirmation in current and any proposed guidance to support the implementation of IPP3A in the HIPC that the 3A(4)(d) exception permitting non-compliance with notification requirements '*to avoid prejudice to the maintenance of the law by any public sector agency*' is not limited to public sector agencies. It can be accessed by individuals and/or other agencies that participate in public agency processes, investigations or prosecutions.

Context in which MPS receives health information

3. MPS is a mutual society, that protects and supports the professional interests of its members. Its assistance includes providing advice and support to meet regulatory, professional and legal obligations, and assisting in responding to complaints, regulatory or legal investigations, and prosecutions. MPS may indemnify members for complaints or claims arising from professional practice. For some matters MPS will engage lawyers to assist its members, but in others advice will

[1] MPS is the professional indemnifier for over 85% of medical practitioners in New Zealand.

Level 12, 342 Lambton Quay
Wellington 6011, New Zealand | Aotearoa
PO Box 5530, Wellington 6140, New Zealand | Aotearoa

WOTTON KEARNEY | **WELLINGTON | TE WHANGANUI-A-TARA**
E: newzealand@wottonkearney.com **W:** www.wottonkearney.com
T: + 64 (0) 4 499 5589

be provided directly by members of its technical in-house team of clinically trained medicolegal consultants.

4. In providing assistance, MPS regularly receives — unbidden from members — health information about individuals involved. MPS might also request such information, to enable a complete understanding of context, and an accurate basis to provide effective advice and make indemnity decisions. Within investigations or proceedings, MPS indirectly collects health information through the same being exchanged or produced by other agencies and/or individuals involved.

Currently proposed 3A(4) exceptions insufficient

5. Across the spectrum of assistance MPS provides, there may be circumstances where it can rely on a proposed 3A(4) exception to avoid the notification requirements in 3A(1).

6. By way of example:

(4)(b) Prejudice the purposes of collection

6.1 A driving purpose behind MPS collecting health information indirectly is to ensure it has fulsome information on which to provide accurate, appropriate and efficient advice, support and indemnity to members. There will be circumstances where this purpose would be undermined if the individual concerned was notified by MPS of the indirect collection, including the reason for the same (i.e. to assist and support a member — which could include defending a complaint, claim or investigation arising from care provided to the individual).

4(c) Compliance is not reasonably practicable

6.2 There will be circumstances where it is not reasonably practicable to notify that MPS has indirectly collected and holds health information about an individual, such as where:

(a) the individual is deceased, very unwell or incapacitated;

(b) there are no contact details, or up to date contact information for the individual concerned, or the individual's representative;

(c) MPS involvement may be resisted or unwelcome (where representing/serving the interests of members); and

(d) contact from MPS may be inappropriate, in the context of contested matters or proceedings where the parties are legally represented.

4(d) Non-compliance is necessary to avoid prejudice to the maintenance of the law by any public sector agency

6.3 The Privacy Commissioner's 'Guidance on IPP3A' (**2025 Guidance**) proposes this exception is only available to public sector agencies.[2] It is submitted this is incorrect. The wording of the proposed clause enables a broader application — including to those involved or participating in a public sector agency process, investigation or prosecution. That this interpretation is available has been confirmed by the High Court in *Nicholls v Health and Disability Commissioner* [1997] NZAR 351.

6.4 The rationale underlying this exception is to ensure public agencies can most effectively achieve their legal purposes, for example through preventing, detecting, investigating, prosecuting, and punishing offences. Where MPS is involved in assisting a member in any such public agency task, and indirectly receives health information about an individual, there would be circumstances where notifying of that collection would impact and/or influence how

[2] Privacy Commissioner 'Guidance on IPP3A – Notification requirements for indirect collection of personal information' October 2025 <20251216-IPP3A-guidance-finalised-for-web-A1135067.pdf> (**2025 Guidance**) at 14.

an individual engages. This in turn could influence the thoroughness and/or accuracy of information available to the public agency.

6.5 The scope of the application of this exception should be confirmed in the 2025 Guidance (and in the proposed healthcare sector specific guidance) to apply to public sector agencies, and individuals and/or other health agencies that participate in public agency processes, investigations or prosecutions.

4(h)(i) Health information will not be used in a form in which individual is identified

6.6 While this exception would be accessible to MPS, the time and resource required to anonymise health information indirectly received, in order to 'use' it, would be a disproportionate (and sometimes needless) prerequisite.

6.7 The transparency and control justifications underlying 3A — particularly that being achieved by anonymisation — would, in most cases, be undermined where the MPS is vested with information about a situation or matter in various ways, from various sources, at various times. For example, the Health and Disability Commissioner, Accident Compensation Corporation and registration authorities (i.e. the Medical Council) regularly identify complainants or relevant patients in their communications. This is required, for natural justice and for a response to be made. Medical practitioners, and courts and tribunals also — in responses and/or submissions and/or proceedings — identify individuals in association with their health information. Any protections achieved by MPS anonymising that health information after collection, in the course of its use or regard to it in this context, would be entirely artificial.

6.8 MPS having an objective and full understanding of the particular circumstances of a case/matter, including through the collection of health information, is necessary for appropriate coverage decisions. Due to this, relevant health information is indirectly collected by MPS in almost every case. As well as being ineffective protection, in the context described in paragraph [6.7], anonymising the information collected would impact on the efficiency of support and assistance, and resolving matters. It would require significant resource to implement, and inevitably, drive up the cost of indemnity cover generally.

6.9 Vesting the anonymising task with MPS members would also come with consequences. Medical practitioners are overburdened, time poor, and will often have no access to readily available and high-quality support — beyond MPS. Requiring a practitioner, in need of help, to find time to anonymise health information (often a significant volume of clinical records) would be a barrier to accessing support.

7. It is submitted the piecemeal application and described implications of the currently proposed exceptions — against the benefits that underly the services provided by insurance/indemnifying agencies, such as MPS — justify a further exception being included in 3A(4) of the HIPC.

New 'maintenance of the law' exception

8. The HIPC recognises the important role of organisations that provide insurance/indemnity services in the healthcare context, and the relevance, and receipt of individuals' health information by such agencies.[3]

9. It is in the interests of justice and society that medical practitioners can seek help/assistance with complaints, concerns or matters raised related to the provision of healthcare. MPS involvement furthers justice and is in the interests of society through, for example:

9.1 promoting and enhancing public benefit through assisting and/or ensuring medical practitioners meet regulatory, professional and legal compliance obligations;

[3] Refer HIPC, s 4(2)(h).

9.2 promoting efficiency, through the involvement of expert advisors and resources to identify and allocate any risk and/or fault — and proposing and/or supporting resolution on that basis;

9.3 assisting medical practitioners to appropriately and comprehensively respond, while maintaining safety standards (through the provision of required support and/or advice); and

9.4 facilitating access to redress through facilitating funds to satisfy judgments or settlements, substituting costs being borne by the medical profession as a whole.

10. MPS having a thorough understanding of the particular circumstances of a matter, including through the collection and consideration of relevant health information, is necessary to achieve the above.

11. Securing the ability for indemnifiers and advisors to receive health information indirectly in the course of the important work of providing claims management services and/or advice and/or legal advice to healthcare providers, without risk that may accompany notification of that collection, could be achieved through a 3A(4) exception on the following terms:

> *(4) It is not necessary for a health agency to comply with subrule (1) if the health agency believes, on reasonable grounds,—*
> *…*
> *(d) that non-compliance is necessary—*
> *…*
> *(ii) to avoid prejudice to the maintenance of the law where information is collected by an indemnifier or adviser for the purposes of claims management services and/or advice and/or legal advice to healthcare providers …*

12. It is submitted appropriate to prioritise the 'interests of justice and society' rationale over the interests of those whose health information is indirectly collected by indemnity providers — like MPS — where any implications arising from indemnifiers collecting that information, for the limited purposes of its involvement, would have little, if any, substantive or lasting privacy implications.

Conduct of proceedings exception

13. The following exception to notifying of the indirect collection of health information will be incorporated into the Privacy Act 2020 from 1 May 2026:

> *(c) that non-compliance is necessary—*
> *…*
> *(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation) …*

14. The Privacy Commissioner proposes not to incorporate the above into the HIPC, on the basis it is considered "*unlikely*" the exception would be relevant or justify not notifying an individual of the indirect collection of health information by a health agency.[4]

15. It is submitted the 'conduct of proceedings' exception is — in fact — important to include in 3A(4) of the HIPC. Court and tribunal proceedings must be informed by all relevant information, and in the interests of justice, there must be no barriers or risk to this.

16. Where MPS is involved in assisting a member in court or tribunal proceedings, and indirectly receives health information about an individual, MPS notifying the individual of the collection could have a material detrimental impact. An awareness of the involvement of an indemnifier, and associated expert support, could escalate tensions and the perception of the seriousness of a matter. It may stifle a desire to participate, or it could prompt important relevant information being interfered with,

[4] Privacy Commissioner *Information paper 4 – Adding rule 3A to the Health Information Privacy Code 2020* <20260108-IPP3A-HIPC-Information-Paper-A1150470.pdf> at 5.

impacting the thoroughness and accuracy of the information base available in the course of proceedings.

17. It is submitted the following should be included in 3A(4)(d):

> *(4) It is not necessary for a health agency to comply with subrule (1) if the health agency believes, on reasonable grounds,—*
>
> *…*
>
> *(d) that non-compliance is necessary—*
>
> *…*
>
> *(iii) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation).*

Concluding comments

18. We and MPS are grateful for the Privacy Commissioner's consideration of the submissions above. We are happy to meet to discuss this submission, or to provide further information.

Yours sincerely

Kate Wills
Senior Associate
D: [redacted]
E: [redacted]

Adam Holloway
Partner
D: [redacted]
E: [redacted]

From: [redacted]
To: IPP3A; [redacted]
Cc: [redacted]
Subject: RE: Privacy code of practices - incorporating Information Privacy Principle 3A
Date: Friday, 13 February 2026 5:36:51 pm
Attachments: image001.png

Kia ora OPC team

Thank you for the opportunity to provide a submission, on behalf of Experian, on the proposed changes to the Credit Reporting Privacy Code to add a new rule 3A.

Experian is supportive of the proposed updates to the Code. However, we would like to suggest further details being included in the Guidance Note in Schedule 3 (Subscriber Agreement). This is to address our concern that the current Guidance Note could cause confusion as to the Privacy Commissioner's expectations on the relationship between Subscriber Agreements and Rule 3A. Our suggestion would be something along the line of the following (with additions show as underlined):

> ***Guidance Note***
> *"The requirements in this Schedule do not limit or replace a credit reporter's obligations under rule 3A. A subscriber agreement may impose additional obligations on a subscriber that are not set out in this Schedule, including to reflect rule 3A. For example, as part of a credit reporter's practices to rely on rule 3A(4), a subscriber agreement may require the subscriber to ensure that, where the subscriber collects credit information directly from the individual concerned, the individual has been made aware of the matters specified in rule 3A(1) in relation to the credit reporter's collection of their personal information. However, a subscriber agreement cannot require the subscriber to satisfy rule 3A(2) (website statement) on behalf of the credit reporter."*

Our suggested additions to the Guidance Note reflects the practical relationship between credit reporters, subscribers and individuals. In general, a credit reporter does not have a direct relationship with the individual and so will hold on very limited contact details. A subscriber (commonly a credit provider) as the owner of the relationship with the individual is best placed to ensure that the individual has been made aware of the matters specified in Rule 3A(1). This approach is also consistent with the principle of data minimisation i.e., a credit reporter is generally precluded from and would not want to collect further contact details solely for the purpose of satisfying Rule 3A (as discussed in the OPC's *Guidance on IPP3A: Notification requirements for indirect collection of personal information* on page 24). We assume that this aligns with the OPC's view, however, it would be useful for the Guidance Note to directly address this.

Thank you again for the opportunity to consult and we are happy to discuss any questions.

Kind regards

Stephen Blyth
Head of Compliance & Privacy
Australia & New Zealand

Experian Australia Pty Limited
Level 14, 2 Southbank Boulevard | Southbank | Vic | 3006
Phone: [redacted]

From: IPP3A <IPP3A@privacy.org.nz>
Sent: Wednesday, December 17, 2025 11:41 AM
To: [redacted]
Subject: [EXTERNAL] Privacy code of practices - incorporating Information Privacy Principle 3A

Tēnā koe

The Privacy Amendment Act (the Act) received Royal Assent on 23 September 2025 and comes into force on 1 May 2026. The key change in the Act is the creation of a new Information Privacy Principle 3A (IPP3A). IPP3A changes an agency's obligations when collecting personal information indirectly, meaning where an agency collects personal information from someone other than the person themself.

The Office of the Privacy Commissioner currently has seven codes of practice in force. We are reaching out to you as we are progressing work on how to amend the codes of practice to incorporate IPP3A. As part of this process, we are intending to commence formal consultation on proposed amendments to the codes from **Monday 12 January 2026** to **Monday 16 February 2026**.

We are currently finalising consultation documents which will be made available on our website on **Monday 12 January 2026**. We are particularly interested in hearing from stakeholders covered by the codes of practice we are proposing to amend to ensure they are workable and meet the policy intent of IPP3A. You are welcome to forward this email to anyone else you know who may have an interest in providing feedback on draft amendments to the codes.

If you have any questions before formal consultation commences, please email IPP3A@privacy.org.nz, and we will get back to you.

Ngā mihi
Craig

Craig McWilliams
Senior Policy Adviser |

Office of the Privacy Commissioner Te Mana Mātāpono Matatapu
PO Box 10094, Wellington 6011
E [redacted]
privacy.org.nz

CENTRIX
Credit Bureau of New Zealand

16 February 2026

IPP3A Codes Team
Office of the Privacy Commissioner

via email: IPP3A@privacy.org.nz

IPP3A: Proposed amendments to the Credit Reporting Privacy Code 2020 (CRPC).

1. Thank you for the opportunity to provide submissions on the changes to the CRPC required due to the creation of IPP3A. Centrix is one of the three consumer credit reporters in New Zealand governed by the CRPC.
2. During information engagement with the OPC Centrix provided substantial submissions on proposed amendments to the CRPC and for efficiency, we will not repeat them other than to confirm our previous submissions.
3. We respond on some other matters arising from the draft CRPC provided for consultation:
    a. We consider all the exceptions in the draft CRPC are appropriate and should remain, noting the OPC is seeking to broadly to align the Codes with IPP3A.
    b. Given the passage of time, Schedule 9 is redundant and we invite the Commissioner to take this opportunity to remove the Schedule.
4. Thank you for the opportunity to provide feedback on IPP3A and amendments to the CRPC. Please do not hesitate to contact me if you have any questions.

Yours faithfully

Keith McLaughlin | Managing Director
Centrix Group Ltd

CENTRIX
Credit Bureau of New Zealand

23 October 2025

IPP3A Codes Team
Office of the Privacy Commissioner

via email: IPP3A@privacy.org.nz

IPP3A: Credit Reporting Privacy Code 2020 (CRPC) changes

1. Thank you for the opportunity to provide submissions on the changes to the CRPC required due to the creation of IPP3A. Centrix is one of the three consumer credit reporters in New Zealand governed by the CRPC.

2. Given the operational impact IPP3A in its current form will have on credit reporters, we request the Commissioner undertakes consultation meetings with the credit reporters and other interested groups on the proposed changes to the CRPC before a draft CRPC is issued for consultation.

3. As you will be aware, credit reporters are trusted third parties holding sensitive financial information, performing a vital role in the consumer credit ecosystem. Generally, a credit reporter collects and provides credit information to its subscribers for the purpose of assisting its subscribers to make decisions relating to the creditworthiness of a consumer (including for debt collection purposes), decisions relating to the underwriting of insurance, tenancy or employment and for AML/CFT compliance.[1]

4. Credit reporters collect large amounts of credit information indirectly and in very limited circumstances do they collect information directly from consumers.

5. In summary Centrix submits that:

   a. The requirements of IPP3A should not be incorporated into the CRPC, with the CRPC already having adequate notification and accountability requirements and controls to achieve the purposes of IPP3A.

   b. Credit reporters have been collecting credit information indirectly for many years, with the first CRPC introduced around 20 years ago that included notification requirements by subscribers of credit reporting services. This requires a subscriber agreement to be in place with all subscribers that includes an obligation on subscribers to notify consumers about the indirect collection of credit information by credit reporters.

   c. In most instances when collecting information from a subscriber the individual has authorised the collection, and the individual is aware of the collection.

[1] See the CRPC for the strict requirements and purpose of disclosure of credit information.

Level 4, 56 Cawley Street, Ellerslie, Auckland, 1501 ▪ P.O. Box 62512, Auckland, 1546
Phone: +64 9 9669706

d. Notwithstanding the above, if the Commissioner considers IPP3A should be incorporated into the CRPC, Centrix submits:

   i. there should be no requirement to notify the name and address of the credit reporter but a requirement to notify the information may be disclosed to a "credit reporter"; and

   ii. any notification requirements in addition to those currently in the CRPC should be added to the current subscriber notification requirements in Schedule 3 to the Code.

Information credit reporters collect

6. In most instances credit reporters do not collect credit information directly from the individual. The general exceptions are when an individual requests access to or correction of their credit file, or seeks a suppression of their credit file.[2]

7. The type of information a credit reporter can collect in its credit reporting function is strictly prescribed in the CRPC and a credit reporter cannot collect any other information for its credit reporting functions.

8. Credit reporters collect credit information primarily from the following sources:

   a. **Subscribers** (such as credit providers, insurers, landlords, employers, insurers, debt collectors). This includes name, address, sex, date of birth and depending on the type of subscriber can include information about employment, driver licence details, credit applications, defaults, credit account information and repayment history (known as CCR), serious credit infringement and credit non-compliance action.

   b. **Public registers and sources** (such as Companies Office, Insolvency Register, Tenancy Tribunal, PPSR). This includes information about directorships and shareholdings, debt repayment orders, judgements for monies, insolvency information, limited partnership information and registered security interests.

9. To give the Commissioner a sense of the volume of credit information collected by Centrix, currently, Centrix holds information on over 95% of the credit active population in New Zealand, being just over **4 million** people. Given this number of consumers, it is not operationally tenable for Centrix to notify individuals of indirect collection of credit information from 1 May 2026. To explain some of the issues that would result in significant increased costs and time:

   a. The notification process would involve a number of manual tasks;

   b. While Centrix holds some email addresses for consumers, most of the notifications would have to be sent by post; and

   c. Due to the variations in the type of credit information collected, and for many consumers the collection is from different subscribers that change over time, a "once only" notification from Centrix to a consumer is unlikely to meet the IPP3A notification requirements.[3] This is also likely to lead to notification fatigue by consumers.

10. While Centrix holds the firm view that it is not reasonably practicable for it to comply with the notification requirements of IPP3A, it is not confident that it can rely on the "*not reasonably practicable in the circumstances of the particular case*" exception. Taking

[2] Note in these circumstances, Centrix only uses this information in its credit reporting services where the consumer has sought access to their credit file and the consumer consents to Centrix keeping the information for this purpose.

[3] Noting further guidance on this may be provided by the OPC.

into account the draft OPC guidance[4] on this exception, at this point in time, Centrix considers it may be unable to meet the high threshold requirement in each instance. This would require a consideration of the exception for each collection – the time and cost involved in this would defeat the purpose of relying on the exception. Centrix could not take on the risk of non-compliance by relying wholesale on the "*not reasonably practicable in the circumstances of the particular case*" exception.

No need for additional transparency or oversight on indirect collection by credit reporters

11. Centrix submits IPP3A should not apply to the collection of credit information by a credit reporter and the IPP3A requirements should not be incorporated into the CRPC. The purposes of the new notification requirements are already being met due to:

    a. Existing credit reporting processes and in many cases the individual has given consent to the collection;

    b. The current CRPC already addresses the objectives IPP3A seeks to achieve;

    c. A significant portion of the credit information collected is sourced from public registers (which is excluded from the notification requirements); and

    d. There is already broad public awareness of credit reporting and significant information in the public domain about the three national credit reporters, their contact details, rights of access and correction to a consumer's credit file and the CRPC generally.

Existing processes, consent, notification requirements and CRPC obligations

12. In most cases, where Centrix collects credit information from a subscriber, the subscriber has obtained the consent of the individual to the information being provided to Centrix and Centrix relies on rule 2(2)(b). The individual is aware of the indirect collection by Centrix.[5]

13. The CRPC requires credit reporters to ensure subscribers provide consumers with notification information when subscribers collect credit information (directly or indirectly) for disclosure to a credit reporter.[6] This does not include all the information required by IPP3A, however, the notification requirement includes the purposes for which the credit reporter is collecting the information and the purposes for which the information will be used and disclosed.[7] This essentially covers notification requirements IPP3A (1)(a) – (c).

14. What are the "gaps" in the existing CRPC notification requirements vs the IPP3A notification requirements? These are[8]: name and address of credit reporters, whether the collection of the information is authorised or required by law, and access and correction rights. Centrix submits the CRPC currently includes additional transparency requirements on credit reporters that fill in these "gaps". A credit reporter must:

[4] Privacy Commissioner, Draft guidance on IPP3A, released 29 April 2025.
[5] Generally, Centrix relies on rule 2(2)(a) when collecting credit information from its subscribers. The exception to this is collecting credit information from its debt collector subscribers where Centrix relies on Rule 2(2)(f).
[6] By having certain obligations in the subscriber agreement, CRPC, Schedule 3 clause 1.
[7] CRPC, Schedule 3, clause 1.
[8] IPP3A (1)(d)-(f).

a. conspicuously display on its website a statement setting out the purposes for which it collects credit information and the purposes for which the information will be used. All credit reporters have privacy statements on their website that cover the "gaps";[9]

b. conspicuously display on its website a copy of the Summary of Rights and all official translations released by the Privacy Commissioner. The Summary of Rights includes all notification information (although does not expressly deal with IPP3A(1)(e));[10]

c. provide a copy of the Summary of Rights to consumers in certain circumstances.[11]

15. The Privacy Act (including the new IPP3A principle) does not impose similar additional obligations on other agencies when they collect information indirectly.

Information sourced from public registers

16. As set out in paragraph 8b above, a large portion of the credit information indirectly collected by credit reporters is sourced from publicly available registers, which IPP3A excludes from the requirement to provide notification.

Significant public awareness of credit reporters

17. There is significant public awareness about credit reporters, who they are and their contact details, what information they collect, what is a "credit file" and the rights of access to and correction of credit information. Some examples:

a. The OPC website has a page dedicated to credit reporters;

b. The NZ Government website also has a page dedicated to credit reports, including information on the 3 national credit reporters, the information that is included in a credit report and how consumers can check their credit file.

c. There are a number of other organisations that provide general information to the public about credit reporters and the information they collect. A quick internet search on credit reporters will produce many results, such as the banking ombudsman, financial ombudsman, community law, consumer protection, money hub.

d. The three credit reporters are easily identified when searching "credit reporters" and "credit file nz" on the internet.

18. The consumer awareness of rights of access and correction can be seen in the increase in access requests received by Centrix over the past 5 years:[12]

2025 – 210,747
2024 – 182,070
2023 – 162,277
2022 – 114,371
2021 – 81,485

19. Based on the current year's trends, we are looking at getting close to 240,000 for the 2026 reporting year. This demonstrates that the access rights are known, simple & accessible.

[9] CRPC, rule 3(2).
[10] CRPC, clause 7(4).
[11] CRPC, rules 6(5), 7(4), clause 7(3)
[12] As reported to the OPC in each Assurance Report for those years – each year is for 12 months to 30 June.

20. In addition, the CRPC includes strict assurance requirements, safeguards and regulatory oversight for credit reporters that other agencies are not subject to:

    a. The CRPC requires credit reporters to undertake monitoring of its subscribers for compliance with the Schedule 3 subscriber obligations and to identify and investigate possible breaches of the subscriber agreement. This includes a requirement for credit reporters to monitor subscribers for notification requirements[13].

    b. The CRPC requires credit reporters to file an assurance report with the OPC providing assurances on the credit reporter's compliance with the CRPC. These reports are made available on the OPC website[14].

21. Simply incorporating the IPP3A amendments into the CRPC ignores the current credit reporting regulatory framework that is working well and already provides assurance requirements and significant oversight and ensures transparency. There is no need for IPP3A to be added to an already satisfactory regulatory regime.

Requirement to name credit reporter not necessary and is a barrier to switching providers/new entrants

22. If the Commissioner considers the notification requirements for credit reporters should be incorporated into the CRPC, Centrix submits it is not necessary for the notification requirement to include the name and address of the credit reporter. The requirement should be to provide a general description (for example "credit reporter"), as requiring a name is likely to increase the barriers for subscribers wanting to change its credit reporting supplier, thereby reducing competition, which will ultimately be to the detriment of subscribers and consumers.

23. As discussed above, there is a wealth of public information available on the names and contact details of the three national credit reporters.

24. If a bank or finance company is required to list by name the credit reporter/s it intends sharing information with, it has the following options available to it:

    a. do nothing if it already names its current supplier/s of credit reporting services;

    b. update its notification information to list its current supplier/s of credit reporting services; or

    c. update its notification information to list all three current credit reporters to ensure they have "covered all the bases". This may confuse the consumer, and raises issues about whether this type of notification achieves the purposes of IPP3A.

25. If at a later date the bank or finance company wishes to switch credit reporters, or decides to share credit information with another credit reporter, or a new credit reporter enters the market, it will have to notify all of its customers of the change, as well as updating all its documentation (which will require significant time and resource). The time and cost of doing this is likely to be a factor in the bank/finance company's decision about whether to switch credit reporters and may result in the bank/finance company staying with its current supplier. This notification requirement provides a barrier to competition between the credit reporters, as well as any new entrants to the market.

[13] CRPC, rules 2(d), (e) and (f).
[14] CRPC, clause 7.

Incorporating IPP3A into the CRPC

26. If the Commissioner considers IPP3A must be incorporated into the CRPC, Centrix submits the CRPC is amended as follows:

    a. the notification requirements are added to the current subscriber notification requirements in clause 1 of Schedule 3 – this is the most sensible option given the current notification requirements in the CRPC and the relationship the subscriber already has with the consumer;

    b. the CRPC expressly provides a credit reporter is not required to notify an individual of an indirect collection if a credit reporter reasonably believes the collection of credit information is from a subscriber who has entered into a subscriber agreement that the complies with Schedule 3 (noting that this is already the definition of subscriber agreement in the CRPC); and

    c. all other exceptions in IPP3A are incorporated into the CRPC.

27. To assist the Commissioner, in Schedule 1 we provide a proposed draft of Rule 3A and amendment of Clause 1 of Schedule 3 reflecting the submission in paragraph 25 above.

Centrix' primary submission

28. We have provided the Commissioner with alternative submissions, however Centrix' primary view is that the requirements of IPP3A should not be incorporated into the CRPC. As discussed above:

    a. in most cases the individual has consented to the collection by Centrix from a subscriber;

    b. the CRPC already has adequate notification and accountability requirements and controls to achieve the purposes of IPP3A; and

    c. there is already broad public awareness of credit reporting and significant information in the public domain about the three national credit reporters, their contact details and access and correction rights to a consumer.

29. Thank you for the opportunity to provide feedback on IPP3A and amendments to the CRPC and we look forward to discussing this with you when carrying out consultation on the proposed changes. Please do not hesitate to contact me if you have any questions.

Yours faithfully

Keith McLaughlin | Managing Director
Centrix Group Ltd

CENTRIX
Credit Bureau of New Zealand

SCHEDULE 1

Note:

1. We have highlighted those parts that differ from IPP3A, other than the replacement of "agency" with "credit reporter" and "information" with "credit information"
2. We have included the notification requirement IPP3(1)(d) name and address of credit reporter, however, Centrix submits this is not necessary.

The Code is amended by inserting the following after Rule 3

Rule 3A

Collection of credit information other than from individual concerned

(1) If a credit reporter collects credit information about an individual other than from the individual concerned, the credit reporter must take any steps that are, in the circumstances, reasonable to ensure that the individual concerned is aware of—

(a) the fact that the information has been collected; and

(b) the purpose for which the information has been collected; and

(c) the intended recipients of the information;

(d) the name and address of-

i. the credit reporter that has collected the information; and

ii. the credit reporter that is holding the information; and

(e) if the collection of the information is authorised or required by or under the law, the particular law by or under which the collection of the information is authorised or required; and

(f) the rights of access to, and correction of, credit information held by the credit reporter provided under rules 6 and 7.

(2) The steps referred to in subrule (1) must be taken as soon as is reasonably practicable after the information has been collected (unless taken sooner).

(3) A credit reporter is not required to take the steps referred to in subrule (1) in relation to the collection of credit information if:

(a) the individual concerned has previously been made aware by any means of all the matters specified in subrule 2 in relation to the credit reporter's collection of the information; or

(b) the credit reporter reasonably believes the collection of the information is from a subscriber who has entered into a subscriber agreement.

(4) It is not necessary for a credit reporter to comply with subrule (1) if the credit reporter believes, on reasonable grounds,-

(a) that non-compliance would not prejudice the interests of the individual concerned; or

(b) the information is publicly available information; or

(c) that non-compliance is necessary-

i. to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences; or

ii. for the enforcement of a law that imposes a pecuniary penalty; or

iii. for the protection of public revenue; or

iv. for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(d) that compliance would prejudice the purposes of the collection; or

(e) that compliance is not reasonably practicable in the circumstances of the case; or

(f) that compliance would cause a serious threat to-

i. public health or safety; or

ii. the health or safety of another individual; or

(g) that the information-

i. will not be used in a form in which the individual concerned is identified; or

ii. will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

(5) It is not necessary for a credit reporter to comply with rule (1) if-

(a) the agency collects personal information for the purpose of determining whether the information is of enduring value for general public interest and should be archived for public reference, study, or exhibition; and

(b) compliance is likely to seriously impair that agency's achievement of the purpose in paragraph 6(a).

(6) It is not necessary for a credit reporter to comply with rule (1) if compliance would be likely to prejudice-

(a) the security or defence of New Zealand, the Cook Islands, Niue, Tokelau, or the Ross dependency; or

(b) the international relations of the Government of new Zealand, the Cook Islands or Niue; or

(c) the relations between any of the Governments of-

i. New Zealand; or

ii. the Cooke Islands; or

iii. Niue; or

(d) the entrusting of information to the Government of New Zealand on the basis of confidence by-

i. the Government of any other country or any agency of the Government of any other country; or

ii. Any international organisation.

(7) It is not necessary for a credit reporter to comply with rule (1) if compliance would-

(a) disclose a trade secret; or

(b) be likely to unreasonably prejudice the commercial position of-

i. the person who supplied the information; or

ii. the individual concerned.

Schedule 3 of the Code is amended as follows

Clause 1 is deleted and replaced with the following

Collection of information by subscriber

(1)

(a) Where the subscriber collects credit information directly or indirectly from the individual concerned for disclosure to the credit reporter, the subscriber must inform the individual of the following:

i. the information will be disclosed to a credit reporter
ii. the purposes for which the credit reporter is collecting the information
iii. the purposes for which the information will be used and disclosed;
iv. the intended recipients of the information;
v. the names and addresses of the credit reporters known at the time of the notice that may be provided with the information;
vi. the collection of the information is authorised by the Credit Reporting Code; and
vii. the rights of access to and correction of information held by the credit reporter under the Code.

(b) The subscriber is not required to take the steps set out in subclause 1(a) in relation to credit information disclosed to a credit reporter if the individual concerned has previously been made aware by the subscriber of all the matters set out in subclause (1)(a) in relation to the collection of credit information by the credit reporter.

EQUIFAX®

23 October 2025

IPP3A Team
The Office of the Privacy Commissioner

By Email: IPP3A@privacy.org.nz

Dear IPP3A Team

Subject: Privacy Act IPP3A – Consultation on Credit Reporting Privacy Code Changes

1. Thank you for the opportunity to provide feedback on changes to the Credit Reporting Privacy Code 2020 (**Code**) as a result of the Privacy Amendment Act 2025.

2. We are grateful for this opportunity which we have discussed with the other credit reporting agencies (**CRAs**) in New Zealand, being Centrix and Experian. We understand Centrix and Experian also intend to make submissions. We and the other CRA's consider a joint meeting with the OPC to discuss the Code changes would also be beneficial. We appreciate the short timeframe to have these changes in place by 1 May 2026, and accordingly Equifax will be available to meet at your earliest convenience.

3. Set out below are Equifax's responses to your queries. In particular, you have asked how IPP3A should best be incorporated into the Code. To this end you have asked:
Whether the exceptions in the Act are appropriate for the Code, and why;
Whether you believe there should be fewer exceptions to IPP3A than those in the Act, and why; and
Whether you believe there should be more exceptions to IPP3A than those in the Act, and why.

4. As a preliminary point we note that Rule 3 of the Code differs from IPP3, in that it has an additional requirement as follows:
(2) A credit reporter must conspicuously display on the credit reporter's website a statement that sets out the purposes for which it collects credit information and the purposes for which the information will be used and disclosed.

5. In our view, Rule 3A should contain this same additional requirement that is set out above, for the purpose of being consistent with Rule 3.

6. If the above amendment is made, this covers some of the requirements of 1(a) to (f) of the new IPP3A, which as you know requires the following, unless one of the exceptions apply:
(1)If an agency collects personal information about an individual other than from the individual concerned, the agency must take any steps that are, in the circumstances, reasonable to ensure that the individual concerned is aware of—
(a)the fact that the information has been collected; and
(b)the purpose for which the information has been collected; and
(c)the intended recipients of the information; and
(d)the name and address of—
(i)the agency that has collected the information; and
(ii)the agency that is holding the information; and
(e)if the collection of the information is authorised or required by or under the law, the particular law by or under which the collection of the information is authorised or required; and
(f)the rights of access to, and correction of, information provided by the IPPs.
(2)The steps referred to in subclause (1) must be taken as soon as is reasonably practicable after the information has been collected (unless taken sooner).

7. As well as the addition we noted above, we consider that the exception in s3 under IPP3A should be amended. This currently provides:
(3) An agency is not required to take the steps referred to in subclause (1) in relation to the collection of personal information if the individual concerned has previously been made aware by any means of all of the matters specified in subclause (1) in relation to the agency's collection of the information.

8. We consider this should be amended to reflect that not every matter in subclause (1) needs to be advised by the collecting agency, if this information is included on the credit reporter's website, as follows:
(3) A credit reporter is not required to take the steps referred to in subclause (1) in relation to the collection of personal information if the individual concerned has previously been made aware by any means of all of the matters specified in subclause (1) in relation to the credit reporter's collection of the information, or the credit reporter reasonably believes it has been named by the collecting agency and the credit reporter displays the matters specified in subclause (1) on its website.

9. We consider that Schedule 3 of the Code, which contains the required terms in a subscriber agreement, should also be amended. Section 1 of Schedule 3 currently provides:
Collection of information by subscriber
(1) Where the subscriber collects credit information directly or indirectly from the individual concerned for disclosure to the credit reporter, the subscriber must inform the individual of the purposes for which the credit reporter is collecting the information and the purposes for which the information will be used and disclosed.

10. We suggest Schedule 3 be amended with the wording in square brackets as follows:
Collection of information by subscriber
(1) Where the subscriber collects credit information directly or indirectly from the individual concerned for disclosure to the credit reporter, the subscriber must inform the individual of the [name of the credit reporter, the] purposes for which the credit reporter is collecting the information and the purposes for which the information will be used and disclosed.

11. In our view, the above changes to the Code, maintain the goal of transparency in relation to the indirect collection of credit information, while allowing a pragmatic and workable approach to achieving this. We consider the remaining provisions of IPP3A are appropriate to be carried through to the Code without further changes.

12. As noted above, we would be grateful of the opportunity to meet with the IPP3A Team, together with the other CRAs, to discuss the Code changes.

We look forward to hearing from you.

Yours faithfully

DRM

Deborah Malaghan
Head of Legal, NZ
Equifax New Zealand Information Services and Solutions Limited