Australian Government

Office of the Australian Information Commissioner

Exposure Draft: Health Legislation Amendment (Data-matching) Bill 2019

Submission of the Office of the Australian Information Commissioner

oaic.gov.au

OAIC

Contents

Introduction

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to provide comments to the Department of Health (the Department) on the Health Legislation Amendment (Data-matching) Bill 2019 Exposure Draft (the draft Bill).
2. The OAIC is an independent statutory agency within the Commonwealth Attorney-General's portfolio with regulatory responsibility for:
   - privacy functions (regulating the handling of personal information under the *Privacy Act 1988* (Cth) and other Acts)
   - freedom of information functions, including access to information held by the Australian Government in accordance with the *Freedom of Information Act 1982* (Cth)
   - information management functions.
3. The OAIC is the independent regulator for the handling of health information in the Australian government public sector and the private sector.[1] Health information is commonly regarded as one of the most sensitive types of personal information. This is reflected in the Privacy Act, which recognises health information as 'sensitive information'[2] and provides extra protections for its handling.
4. The draft Bill proposes amendments to the *National Health Act 1953* and other legislation to enable data-matching for specified Medicare compliance purposes. Our submission focuses on the two key aspects of the draft Bill:
   a. the proposed new Part VIIIA of the National Health Act, which provides the legislative basis for the proposed data-matching scheme
   b. the proposed amendments to the Privacy Act, which provide for the Information Commissioner's oversight in relation to the scheme.
5. The OAIC is cognisant of the public policy objectives underpinning the draft Bill—in particular, ensuring the integrity and continued sustainability of the Medicare system.[3] However, legislation authorising the collection, use and disclosure of personal sensitive information should strike an appropriate balance to ensure any impacts on privacy are reasonable, necessary and proportionate, having regard to the relevant policy objective. The recommendations that we have set out in this submission may assist to calibrate these important public policy objectives in the implementation of the data-matching scheme.

Legislative instrument for data-matching requirements

6. Clause 132F of the draft Bill provides that the Chief Executive Medicare (CEM) must establish and maintain 'systems and processes' to ensure that the matching of information by the CEM—or the Commonwealth agencies they authorise—is in accordance with Part VIIIA of the National Health Act.

[1] For the definition of 'health information' see s 6FA of the *Privacy Act 1988.*

[2] *Privacy Act 1988* s 6.

[3] Department of Health, Consultation Guide, The Health Legislation Amendment (Data-matching) Bill 2019 and Associated Regulations (the Consultation Guide), page 1: consultations.health.gov.au/provider-benefits-integrity/draft-health-legislation-amendment-data-matching-b/.

7. We consider that requirements for compliance with Part VIIIA should be instead provided in a legislative instrument (if it is not feasible to provide the requirements in primary legislation) to ensure appropriate scrutiny and accountability.[4] Importantly, this would also provide additional protection against 'function creep'— that is, collecting, using or disclosing personal information over time in ways that may not have been originally intended, or which may not be reasonable, necessary and proportionate in light of the relevant policy objectives.
8. The OAIC also considers it appropriate for the draft Bill to name the Minister as the office-holder empowered to make the legislative instrument. Although the existing provisions of the National Health Act would enable the Minister to delegate this proposed power to the CEM, [5] formally placing this power with the Minister would invoke greater accountability and scrutiny in relation to the legislative instrument and the data-matching scheme as a whole. Naming the Minister in this regard will also ensure consistency with existing provisions of the National Health Act. [6]
9. We further recommend that the mandatory consultation requirement in subclause 132F(3)—whereby the CEM must consult with the Information Commissioner in establishing systems and processes—should instead apply to the Minister in making a legislative instrument. Generally, we welcome such a consultation requirement and recommend an additional requirement to the effect that the Minister/CEM must have regard to the Information Commissioner's submissions.[7]
10. As a safeguard to accompany the requirements set out in 'systems and processes', the Department has committed to adopt the *Guidelines on data matching in Australian Government administration* issued by the Information Commissioner (the Guidelines).[8] In our view, these Guidelines—operating in conjunction with the 'systems and processes'—would not provide privacy protections commensurate to the safeguards provided by legislative instrument. In particular, the Guidelines are voluntary and there are no specified consequences for breach, unless the conduct also constitutes a breach of an Australian Privacy Principle.
11. We also advise that the Information Commissioner may not maintain the Guidelines in their current form. The National Archives of Australia have recently revoked the records disposal authority for data-matching that underpins the Guidelines in relation to records destruction (Guideline 7).[9] Consequently, the Information Commissioner is currently reconsidering the Guidelines—in particular, how they align with the Privacy (Australian Government Agencies – Governance) APP Code 2017 and the requirement to conduct Privacy Impact Assessments in accordance with that Code.

---

[4] This is achieved in part through mechanisms such as review by the Senate Standing Committee on Regulations and Ordinances or the Parliamentary Joint Committee on Human Rights.

[5] This delegation power is provided by section 6 of the *National Health Act 1953*.

[6] The *National Health Act 1953* includes a number of provisions that provide the Minister with the power to make a legislative instrument (for example: ss 9B(2), 12(1), 84AAE(3), 98C, 99L). The instances that use the Chief Executive Medicare relate to administrative decisions (for example, ss 14 and 15 where the Chief Executive Medicare decides eligibility for a particular scheme).

[7] We note, for example, that s 295M of the *Telecommunications Act 1997* provides for such a consultation requirement.

[8] Department of Heath, the Consultation Guide, p 7. The OAIC publishes these Guidelines online at: /www.oaic.gov.au/privacy/guidance-and-advice/guidelines-on-data-matching-in-australian-government-administration/.

[9] The repealed records disposal authority is *General Disposal Authority 24: Records Relating to Data Matching Exercises*. The National Archives of Australia's General Records Authorities (GRAs), including revoked GRA 24, are available at: www.naa.gov.au/information-management/records-authorities/types-of-records-authorities/GRA/index.aspx.

Balancing policy objectives to ensure proportionate privacy impacts

12. We recommend a provision to the effect that the Minister/CEM be required to consider whether the legislative instrument, or systems and processes, are reasonable, necessary and proportionate to relevant objectives underpinning the data-matching scheme.
13. We note that subclause 132F(2)(a) introduces a proportionality principle in the draft Bill. The subclause requires that systems and processes must ensure that only 'reasonably necessary' information is matched. Consistent with our recommendation above, we consider that such a principle should also be applied at a more foundational level—by the Minister when making legislative-instrument requirements (or the CEM when establishing systems and processes). This helps ensure that the data-matching scheme as a whole (and not only particular instances of data-matching) has an impact on individuals' privacy that is proportionate to the legitimate policy objectives underpinning the scheme.
14. In the alternative, a public interest test may have a similar effect—that is, provisions requiring the Minister/CEM to consider whether the instrument/systems are in the public interest (including public interest factors such as those relevant to the scheme objectives and an individual's right to privacy).

'Terms and conditions'—interaction with consultation requirement and s 33C of the Privacy Act

15. The draft Bill provides for 'terms and conditions' at subclauses 132B(3)–(4). 'Terms and conditions' are determined by the CEM and apply to Commonwealth entities authorised to match information on the CEM's behalf.
16. It is unclear how the CEM's 'terms and conditions' interact with the CEM's 'systems and processes'—in particular, the range of expected content in the 'terms and conditions' and why these are distinct from 'systems and processes'.
17. In the event that requirements for compliance with Part VIIIA are to be set out in 'systems and processes' (and not in a legislative instrument in accordance with our recommendation) we recommend that the draft Bill clarify this interaction, particularly given:
    a. the proposed requirement for consultation with the Information Commissioner in establishing 'systems and processes' but not in determining 'terms and conditions' (clause 132F(3))
    b. the proposed addition to s 33C(1) of the Privacy Act concerning the OAIC's assessment power (discussed further below). The Information Commissioner's proposed remit—as it relates to Commonwealth entities authorised to data-match—concerns whether the matching of information under Part VIIIA, and the handling of information relating to the matching, is in accordance with the CEM's 'terms and conditions' in addition to 'systems and processes': subclause 33C(1)(f)(i)–(ii).
18. More generally, it is our preference that the drafting of the amendment to s 33C be broadened to refer to Part VIIIA—with the legislative instrument/systems and processes made under this part specifically included—to ensure the OAIC will be able to conduct assessments of the handling of information under all relevant provisions.

Exception to s 135AA of the National Health Act and rules

19. We note that the draft Bill proposes an exception to s 135AA of the National Health Act and the rules made by the Information Commissioner as required under this section (the National Health (Privacy) Rules 2018: the s 135AA Rules). Section 135AA and the s 135AA Rules restrict the linkage of information concerning claims for payment/benefits under the Medicare Benefits and the Pharmaceutical Benefits Programs. The policy intent is to recognise the sensitivity of health information, as such linkages may reveal detailed information on individuals' health status and history.

20. It is our view that the Explanatory Memorandum for this Bill should set out:

    a. the policy objectives underpinning s 135AA of the National Health Act

    b. the justification for departing from the protections set out in s 135AA and the s 135AA Rules

    c. how the impacts on privacy from this departure is justifiable—that is, reasonable, necessary and proportionate to the objectives underpinning the data-matching scheme

    d. how the privacy safeguards attached to the scheme mitigate these privacy impacts.

21. The PIA for this legislative package should also address the four issues above.

'Interference with privacy' clause and personal information

22. Clause 132E provides:

> A breach of a provision of this Part in relation to an individual constitutes an act or practice involving interference with the privacy of the individual for the purposes of section 13 of the *Privacy Act 1988*.

23. The effect of this provision is to specifically enliven the OAIC's regulatory powers (not limited to the assessments power in s 33C but also in relation to complaints, investigations and determinations). The effect of the words 'in relation to an individual' is to impose an unnecessary limitation on the OAIC's regulatory powers by the introduction of a threshold before a breach of the Part can amount to interference with the privacy of the individual under the Privacy Act.

24. If the provision is limited in this way, it may be difficult for the OAIC to determine whether it has a clear regulatory mandate in some information-handling circumstances. This is because it can be a highly contextual question as to whether information constitutes 'personal information' in the data-matching context.

25. It is therefore our recommendation that the OAIC's regulatory scope should extend to all aspects of information-handling under the proposed Part VIIIA of the National Health Act. The objective is not to extend the OAIC's jurisdiction, but rather to eliminate any uncertainty as to whether the OAIC has the power to take regulatory action in the various circumstances where information may not have been handled in accordance with requirements. This would ensure that the transparency and oversight measures in relation to all types of information handled under Part VIIIA are robust and consistent.

26. We note that the PIA executive summary states that nearly all data proposed to be shared or matched will be—or can be—linked to an individual; and that 'data matched for compliance purposes should all be treated as personal information for the purposes of compliance with

the APPs'.[10] We therefore consider broad oversight by the OAIC is appropriate to ensure that community expectations are met in relation to the handling of this information, which is considered especially sensitive and in need of protection (as discussed above).

27. An unlimited provision would also ensure that the Bill does not reduce the OAIC's current regulatory scope in relation to this information (see the current terms of s 13(5)(b) of the Privacy Act, which provides that any breach of the s 135AA Rules is an interference with privacy).

28. It is our view that this approach also aligns with that taken in relation to the OAIC's oversight role concerning the handling of other sensitive categories of information, for example credit reporting information (which is regulated by the OAIC even in its de-identified form—see s 20M of the Privacy Act). By way of further example, provisions addressing 'interference with the privacy of the individual/healthcare recipient' in the *My Health Records Act 2012* (Cth) and the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) are not specifically limited to personal information in the manner proposed by the Bill.[11]

'Interference with privacy' clause and s 13 of the Privacy Act

29. There are no proposed consequential amendments to s 13 of the Privacy Act to reflect clause 132E of the Draft Bill, except for a proposed note at the end of s 13(5) to include this Bill as an example of an Act that provides that an act or practice is an interference with the privacy of an individual.

30. While not strictly necessary for the operation of clause 132E, we consider that a consequential substantive amendment to section 13 of the Privacy Act—and not just the addition of a note to section 13(5)—would be useful to reduce any ambiguity of the operation of this clause.

Specificity in the instrument/systems and the PIA

31. The legislative instrument or systems and processes should set out data-retention requirements, including how long matched information can be retained as a combined data-set. A specific time-frame is preferable, as it creates certainty, but in the alternative, principles relating to retention may be appropriate (for example, as long as reasonably necessary to achieve an objective with a particular data match).

32. The PIA for this legislative package should also address specific time-frames or principles for data-retention requirements—including for matched information, as discussed above.

33. We also recommend that the PIA set out a full analysis of the information flows, privacy impacts, risks and mitigation strategies (for more information, see our *Guide to undertaking privacy impact assessments*).[12] This should include the Commonwealth agencies that the CEM may authorise to match information under this scheme, and the private-sector entities (in particular private health insurers) that may provide information to the CEM.

---

[10] King & Wood Mallesons, Galexia, *Department of Health, Privacy Impact Assessment (PIA) for the Data Matching Proposal, PIA: Fraud detection and compliance activities, 2019*: Executive Summary, page 8: consultations.health.gov.au/provider-benefits-integrity/draft-health-legislation-amendment-data-matching-b/.

[11] *Data-matching Program (Assistance and Tax) Act 1990* s 14; *My Health Records Act 2012* s 73(1) (in particular, in relation to contravention of parts 4–5 of that Act).

[12] See, in particular, 'Map information flows' at [5]: www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/.

Conclusion

34. The OAIC is available to provide further information as required.