



SAPPHIRE ICT SYSTEM PRIVACY IMPACT ASSESSMENT: RESPONSE TO RECOMMENDATIONS

PIA Recommendation: APP1 – *The ‘privacy statement’ on the My Profile screenshot for Sapphire should also contain a link to the NHMRC’s Privacy Policy.*

NHMRC response: AGREED

PIA Recommendation: APP1.3 – *[T]he stated reasons for gathering personal information under the NHMRC’s Privacy Policy contains only a relatively brief description of the primary reason for collecting the information. We recommend that a more expansive description of the reasons and the manner of collection through applications be inserted in the policy itself.*

NHMRC response: AGREED

PIA Recommendation: APP 1.4(f) – *[T]he description on page 11 of the [Privacy] Policy (‘Disclosure of Personal Information to Overseas Recipients’), in the first paragraph, be amended to read ‘must be sent overseas or where the assessor or reviewer best suited and available to assess the application is overseas’ – or something similar.*

NHMRC response: AGREED

PIA Recommendation: APP 8 – *Where the particular overseas destination for personal information is not known or disclosed at the time an application is lodged, NHMRC to consider whether it could confirm with an individual their earlier general consent in their application before disclosing personal information to an overseas recipient once the proposed actual overseas destination is known and disclosed to the individual.*

NHMRC response: NOT AGREED

NHMRC arrangements are compliant with APP 8 as NHMRC’s grant systems require explicit agreement that, in accordance with APP 8, consent is given to send personal information overseas, if required, for the purposes of peer-review of an application. NHMRC makes all reasonable efforts to protect personal information, recognising that assessors outside Australia are bound by their own country’s laws and consequently we cannot provide assurance that information will be handled in accordance with the same standards as required by the *Privacy Act 1988*.

PIA Recommendation: APP 10 — Each year, NHMRC should send an electronic reminder to all researchers for whom they hold a cv/researcher profile, recommending that they personally log on and review their cv to satisfy themselves as to its accuracy and whether it is up to date (to address the risks of personal information not being accurate or up to date, and the possible need for information to require correction/inclusion as a result of the data migration process involved in the establishment of Sapphire).

NHMRC response: AGREED

PIA Recommendation: APP 10 — Include, in a prominent place on Sapphire, a notice to individuals urging them to ensure regularly that the personal information that NHMRC holds about them is accurate and up to date.

NHMRC response: AGREED

PIA Recommendation: APP 11 — That the NHMRC's training and delegations/ authorisations regimes for staff and third party contractors using or having access to Sapphire be more formalised, with the training to be institutionalised within the agency's corporate management system. Additionally,a register of training should be maintained, and a register recording the varying levels of access provided to staff and contractors should be maintained.

NHMRC response: AGREED

PIA Recommendation: APP 12 — [E]nsure that any maintenance and upgrade work undertaken by third party [IT] contractors does not provide unrestricted access to the personal information contained in Sapphire unless it is considered absolutely necessary by NHMRC for the purposes of the task those contractors are performing.

NHMRC response: AGREED

PIA Recommendation: APP 13 — NHMRC's Privacy Policy - it would be desirable for the requirements of APP 13.3 re the 30 day deadline for the agency to correct personal information to be noted in the policy itself.

NHMRC response: AGREED