National Health and Medical Research Council

Privacy Impact Assessment Report on the Implementation of the Sapphire System

30 January 2019

For Official Use Only

PREPARATION AND CLEARANCE

Responsibility for the Project

Tony Krizan, CIO and Executive Director, Sapphire Transition Task Force

PIA completed by:

Bruce Brown, Consultant Proximity Legal

Clearance for the Report

Cleared/reviewed by: Tony Krizan

DEFINITIONS

AI – Administering Institution

cv, and researcher profile – in the context of this PIA, the terms 'cv' and 'researcher profile' are effectively interchangeable

APP – Australian Privacy Principle

COI – Conflict of Interest

NHMRC – National Health and Medical Research Council

NHMRC Act – *National Health and Medical Research Council Act 1992*

OAIC – Office of the Australian Information Commissioner

ORCID – 'Open Researcher and Contributor ID' - a unique, open sourced, international identifier system for researchers in various fields, which enables them to disambiguate their name and research activity. Uptake of this facility has been increasing in the research community, although its use is not currently prescribed by NHMRC.

PGPA Act – *Public Governance, Performance and Accountability Act 2013*

PIA – Privacy Impact Assessment

Privacy Act - *Privacy Act 1988*

RGMS – Research Grants Management System

Staff – Staff employed by the NHMRC [*but not including contractors or consultants]*

The term 'Applicant' – The NHMRC manages a range of funding schemes. In all cases, the funding is directed through the research body itself ('Administering Institution'/AI), although in practice the funding is for individual researchers or research teams. In some cases, the applications contain large amounts of personal information about the researcher involved in the research proposal. In this PIA, unless the context suggests otherwise, the reference to an applicant is to a researcher listed in the application lodged by an AI who is either an individual researcher or an individual who is nominated as a member of a research team.

The term 'grant application form' – Each grants program has its own particular rules and application form . In this PIA, unless the context suggests otherwise, the reference to an application form can include all the various application forms used for all the different funding/grant schemes that involve or require the collection of personal information.

INTRODUCTION

Proximity has been engaged by NHMRC to conduct a Privacy Impact Assessment (PIA) review of the implementation of the Sapphire system and provide advice on any potential privacy issues that may need to be addressed during the development and implementation stages of Sapphire.

The instructions for this project provided that the ambit of the PIA was to be limited to an assessment of:

- the application process;
- the research grants process, including the allocation of panel members to assess applications;
- the identification of experts for NHMRC Committees and other external committees/panels;
- internal analytics of any data about commercialisation from NHMRC research funding or applications (not necessarily only those applications which were funded);
- the Privacy notices proposed for Sapphire, and NHMRC's recently revised Privacy Policy; and
- who has access to Sapphire and for what purpose.

Additionally, the instructions clarified that considerations regarding future potential for data sharing with external government agencies and other similar proposals are to be addressed separately at a later date.

EXECUTIVE SUMMARY - METHODOLOGY

In undertaking this PIA, we first reviewed NHMRC's Privacy Policy and other publicly available documents on the agency's website and discussed the project with members of the project team undertaking the implementation of Sapphire. This assisted us in understanding the nature of Sapphire, and what its adoption aims to achieve.

We then drilled down to assess the system against each of the 13 APPs. This involved regular consultation with the project implementation team, and discussions with NHMRC's privacy officers and legal team.A significant amount of time was also spent reviewing project materials such as the Data Migration Design document, and draft documents that have already been prepared pending the introduction of Sapphire – including, for example, screenshots of the consents on the proposed (online) application forms. We also reviewed key documents relating to the existing grants management system (RGMS – see below), such as the 'NHMRC Partnership Projects Scheme Specific Advice and Instructions to Applicants for Applications Received in 2018', because some elements of the existing system's application process will remain the same.

Stakeholder Engagement

To assist in the completion of this PIA, the following persons were consulted and/or their feedback and input sought at various times:

Gerry Doherty, Assistant Director, Grants System

Sam Faulkner, NHMRC Indigenous Advisor

Deborah Lopert and Alice Spurgin, Principal Legal Officers, Legal Services

Alana Lucas, NHMRC Privacy Officer

Marita Sloan, Director, Strategic Projects and Support Section

RECOMMENDATIONS (and some observations)

We found that the implementation stage of Sapphire raises only relatively minor privacy issues that have not already been addressed during the development stage. The PIA process does, however, also involve reviewing an agency's existing Privacy Policy and other privacy documents and, during this process we identified a small number of minor privacy issues that needed addressing more generally.

This PIA Report makes the following recommendations:

APP1	The 'privacy statement' on the My Profile screenshot for Sapphire should also contain a link to the NHMRC's Privacy Policy.
App 1.3	In view of the fact that grants funding and management is the core role of NHMRC, and the collection of personal information is an important aspect of the process, the 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, when an opportunity arises to review the privacy policy, a more expansive description of the reasons and the manner of collection through applications be inserted in the policy itself.
APP 1.4(f)	When an opportunity arises to review the Privacy Policy, the description on page 11 of the 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.
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.
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).

(Another step that NHMRC could take is to 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.)

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, in order to bolster the agency's accountability systems, a register of training should be maintained, and a register recording the varying levels of access provided to staff and contractors should be maintained.

APP 12 That care should be taken to ensure that any maintenance and upgrade work undertaken by third party 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.

APP 13 When an opportunity arises to review the 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, consistently with some other agencies.

Separate Note –Although this PIA is limited to the initial implementation of Sapphire, we note that there are proposals afoot to use more of the capacity of the system in the future, including the following initiatives:

- Future potential for data sharing with other government agencies – a review of any such proposal is specifically excluded from this PIA, but we note it would raise privacy issues and would appear to require a separate PIA if it may involve personal information being disclosed. The proposed data sharing and release legislation currently being considered by the Commonwealth, as well as the statutory powers for each proposed sharing agency would need to be considered carefully in this context.
- Matching information with other databases – these include Trove and IP Australia patent information. This could be seen as a sub set of the above proposal. Matching with information on existing public databases would generally not raise any privacy issues, unless the matching enabled identification of an individual who was previously de-identified within the other database. The likelihood of this occurring would appear to be very low but in any event the matching would need to have a solid legislative underpinning or valid (including at least implied) consent from the individual applying in respect of both (or more) databases.
- Possible future potential for Public Profiles? Depending upon the specific nature of the proposal, this would appear to require some active consent from the individual researchers and with the appropriate controls to be set out as to who can view what information in the profile, and greater specification as to which personal information can be viewed. The potential for this kind of wider use of the personal information held on Sapphire increases the need for ensuring the accuracy and currency of the personal (and in particular sensitive) information held by NHMRC.

We note that the current NHMRC Funding Agreement includes provisions which reserve for NHMRC the right to publicise and report on the awarding of funding to an Administering Institution in multiple ways which can

include information about specified personnel (see cl 21.3 in particular), and the Privacy Policy also contains relevant statements on the disclosure of personal information. Accordingly, there is already a level of underpinning for some of these proposed initiatives, but each of them raises different sets of privacy issues which are outside the ambit of this PIA but which we believe would need to be addressed before any of the initiatives are proceeded with.

Allied to these points, we note there is one matter set out in the formal instructions that we considered only briefly. The fourth dotpoint instruction provided that the PIA was to include (among other things) a review of the following:

- Internal analytics of any data about commercialisation from NHMRC research funding or applications (not necessarily only those applications which were funded).

Sapphire is being developed with an 'outcome reporting application' which in particular would enable NHMRC to data mine and develop case studies of successful grant outcomes, highlighting successful commercialisation outcomes in particular. In principle, and depending upon how wide a view is taken of the consents implied in applications and the conditions contained in the current Funding Agreement, such analysis would be permissible from a privacy perspective. The publicising of this information would arguably be seen as meeting the NHMRC's aim of maximising the benefits arising from any research which the agency funds. In many respects though, this dotpoint issue is better dealt with in a future PIA review addressing all the other data management initiatives referred to above at the same time. We do make one observation at this time, however. There are likely to be significant privacy and other legal barriers to NHMRC undertaking analytics and reporting on outcomes on applications which were ultimately not funded by NHMRC. There would not appear to be a proper legal basis for such 'data mining' or disclosures. The issue may be capable of resolution by inserting an appropriate disclosure statement in the Privacy Policy and in the Funding Agreement in the future.

BACKGROUND

Context: the NHMRC

The NHMRC is established under the NHMRC Act and it is a non-corporate Commonwealth entity within the meaning of the PGPA Act.

The NHMRC's Privacy Policy describes the NHMRC in the following terms:

> NHMRC is Australia's peak body for supporting health and medical research; for developing health advice for the Australian community, health professionals and governments; and for providing advice on ethical behaviour in health care and in the conduct of health and medical research.

Its objects, as set out in section 3 of the NHMRC Act are to pursue activities designed to:

- Raise the standard of individual and public health throughout Australia;
- Foster the development of consistent health standards between the various States and Territories;
- Foster medical research and training and public health research and training throughout Australia; and

- Foster consideration of ethical issues relating to health.[See also the Privacy Policy, p. 4]

In its most recently published annual report, the CEO of NHMRC stated that the organisation 'delivers on the strategic directions of managing investment in health and medical research, developing evidence based health advice, providing advice on ethical practice in health care and the conduct of medical research, and performing functions under the *Research Involving Human Embryos Act 2002* (RIHE Act) and the *Prohibition of Human Cloning for Reproduction Act 2002* (PHCR Act).'

It also has a role under the *Medical Research Future Fund Act 2015* (MRFF Act), in particular that the Commonwealth may draw on NHMRC to deliver research funding from the MRFF scheme, and the *Therapeutic Goods Act 1989* in relation to the registration of Human Research Ethics Committees (HRECS).

Most relevantly for this PIA, the primary role of the NHMRC is the granting and management of research funding in the medical and health research fields. It is a significant health and medical research grants funder and administrator. In the year 2017-18, for example, $943 million was committed in new research grants for individuals, teams, projects and centres in the health and medical research fields (*p. 3. NHMRC Annual Report 2017-18*).

Parliament has adopted a minimalist approach in the NHMRC Act to prescribing how the grants management process should be undertaken. Apart from establishing the Medical Research Endowment Account (MREA) as a special account in Part 7 for PGPA Act purposes, the NHMRC Act itself provides little if any prescription of the process.

NHMRC is, however, subject to the PGPA Act and in particular the Commonwealth Grant Rules and Guidelines 2017 issued by the Department of Finance. Currently, each year, NHMRC submits its funding guidelines/rules to Finance for approval.

More particularly, for the purposes of this PIA, the NHMRC Act is also technology neutral in relation to the form of the IT systems that NHMRC should adopt to undertake its grants management processes.

Context: Privacy Act 1988

As an 'agency' (see subsection 6(1) of the Privacy Act), NHMRC is bound by the Privacy Act in the way it undertakes its functions.

The Privacy Act sets out 13 Australian Privacy Principles (APPs) which regulate the collection, use, storage and disclosure of personal information about individuals by Commonwealth agencies and how individuals can access and correct personal information held about them by those agencies.

Much of the information collected by NHMRC in the course of its grants management processes is personal information, as defined in section 6 of the Privacy Act as follows:

'Personal information' means information or an opinion about an identified individual , or an individual who is reasonably identifiable:

(a) Whether the information or opinion is true or not; and

(b) Whether the information or opinion is recorded in a material form or not.

More specifically, and relevantly for this PIA, much of the personal information collected by NHMRC in the course of undertaking its grants approval and management functions and activities is also sensitive information. 'Sensitive information' is, effectively, a sub- category of personal information. It is defined in section 6 of the Privacy Act to cover a range of matters:

'Sensitive information' means:

(a) Information or an opinion about an individual's:
  (i) Racial or ethnic origin; or
  (ii) Political opinions; or
  (iii) Membership of a political association; or
  (iv) Religious beliefs or affiliations; or
  (v) Philosophical beliefs; or
  (vi) Membership of a professional or trade association; or
  (vii) Membership of a trade union; or
  (viii) Sexual orientation or practices; or criminal record;
  That is also personal information; or
(b) Health information about an individual; or
(c) Genetic information about an individual that is not otherwise health information; or
(d) Biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
(e) Biometric templates.

As a general observation, the Privacy Act imposes higher standards on agencies with respect to the collection, use and disclosure of sensitive information they may hold about individuals.

The NHMRC Act does contain one provision relating to the protection of information which may, in some extended circumstances, be seen as an additional duty on the agency to protect the personal or sensitive information of individuals. Section 80 of the NHMRC Act prescribes offences relating to the disclosure of confidential commercial information. The term 'confidential commercial information' is not defined in the Act and so would be given its ordinary meaning. Nor are the provisions limited to corporate entities (i.e. they could include confidential commercial information relating to an individual which may be seen as personal, and even sensitive, information). From our discussions with NHMRC staff, it appears that such a scenario is highly unlikely because researchers/applicants are never required to provide information about their personal finances for example. Also, it would be highly unlikely that if any such personal financial information were collected, it would be deemed to be 'commercial information' within the ordinary meaning of that term anyway. Accordingly, we did not focus on the requirements of this provision.

Context: The NHMRC Approach to Research Grants Management, and the current Research Grants Management System (RGMS)

Administering Institutions

Each year NHMRC calls for applications for research grants from entities within Australia. Funding out of the MREA is limited to Administering Institutions (AIs) (many of which are universities or established research organisations). A list of these organisations is available at: http://www.nhmrc.gov.au/funding/manage-your-funding/nhmrcs-administering-institutions.

The AI is the organisation that NHMRC primarily deals with in relation to the application and in relation to any subsequent matters relating to the funding and management of any grant that may be awarded. Terms of funding out of the smaller MRFF are for a wider group of potential recipients, but the differences are not relevant for the purpose of this PIA.

Importantly, it is the AI that receives the funding and is effectively the 'managing agent' for the administering of the funds.

Critical elements of any grant application are the identities and 'research track record' of the principal researcher(s) nominated in the application - referred to as Chief Investigator(s). Supporting this person or persons will be a number of nominated research staff, with varying titles (such as associate investigator). Depending upon the particular funding scheme, a significant amount of information about these persons is often provided in the application form lodged by an AI. Much of it is personal, and may be sensitive, information.

Many researchers are named on a number of applications at any one time, and may also be members of project teams that are already being funded. Many researchers also create a digital presence on RGMS and create a cv/profile which are held electronically by NHMRC. They are frequently updated as the individuals, for example, publish new research, receive awards or grants in their individual capacity or as a member of a research team, are promoted, or are appointed to significant committees. These cvs are initially provided voluntarily as part of the grants process. However the monitoring or updating of them is not always undertaken personally by the particular researcher, but by a Research Administration Officer (RAO) within the AI who has been given consent by the researcher to access the cv held by NHMRC and update the information online. Based on the current RGMS database, some 41.1% of researchers have authorised RAOs to have control of, or access to, their cvs/researcher profiles.

It is proposed that, when Sapphire is implemented, the grants application form will include an 'Access to your File' checkbox which the researcher can tick to advise NHMRC that they have given consent for an institution's RAO to have 'edit' access to their cv.

Competition for grants is always strong, and it is important that NHMRC can demonstrate that each grant application was properly considered by a panel of individuals who have relevant expertise in the area of research and who do not have an unmanageable COI. Accordingly, NHMRC uses the cv information it holds on researchers and other experts who have indicated a willingness to be appointed as assessors or panel members. Many of these individuals would be former Chief Investigators on funded grants, and may even be involved in currently funded research, or may be nominated in other grant applications. Clause 23 of the

NHMRC Funding Agreement makes it a condition of funding that an AI must make available the services of 'Specified Personnel' to provide 'professional input' into reviewing or assessing other applications.
There is an element of professional recognition involved in being invited to be an assessor or panel member by NHMRC, and so, for the same reason that an applicant may provide the best picture they can of their experience and abilities in a grant application, cvs may be provided that that could only be described as 'fulsome', within the 100/200 character limits set down for most free text boxes, and the obvious limits of dropdowns from a fixed set of selection options.

Provision of personal information to other organisations

NHMRC may decide to refer an application which has merit but cannot be accommodated in full within its own funding priorities to another (often private) research funding organisation for consideration ('gap funders').

Also, it may undertake a project in partnership with another organisation to fund a particular research project ('co-partnerings'/partnership projects). These may involve the release of a researcher's personal information to a third party.

Funding priorities that require the provision of specific categories of personal (often sensitive) information.

Finally, NHMRC has a number of 'social' imperatives that influence its grants programs, and which have an impact on the kinds of personal/sensitive information that the agency collects.

For example, the current Funding Rules state that a priority area is the improving of gender equality in the rates of awards made to women. [Refer the NHMRC's recently released *Gender Equality Strategy 2018-2021*].

It has also been a feature of NHMRC policy for some time that researchers should have the ability to document legitimate career disruptions without any negative inference being drawn from the interruption to their (research) track record for the purposes of peer reviews. A career disruption involves 'a prolonged interruption to an applicant's capacity to work due to pregnancy, major illness, injury or carer responsibilities.' In peer reviews, an applicant's track record is assessed relative to opportunity, which includes career disruption. In addition, a career disruption may be equally relevant in consideration of appointment as a peer reviewer or member of an assessment panel. [2018 Funding Rules – Career Disruption – Section 6.2.1] [*Refers readers to 'Advice and Instructions for Applicants' and 'Guide to Peer review'] See, as an example relating to grant applicants, para 3.1 CV-D: Career Disruption in the 2018 NHMRC Partnership Projects Advice for Applicants.*

NHMRC also has a stated focus on capacity building among Aboriginal and Torres Strait Islander researchers, who still remain a disproportionately small minority of NHMRC funded researchers. The aim is to attract and support early and mid-career ATSI researchers in particular [See *NHMRC Roadmaps 2 and 3].*

These stated priorities and policies have the practical effect that, depending upon the particular grant framework, researchers will be invited or required to provide sensitive information on matters like gender, race (more particularly indigeneity), and health if they wish to take advantage of the opportunities offered by these stated NHMRC social policies.

The NHMRC Privacy Policy sets out the kinds of personal/sensitive information that it may collect about individuals. Many of these categories are not relevant to the grants management process. Categories of sensitive information that may be collected by NHMRC as part of the grants management process are:

> Sex/gender, physical or mental health, disability status, racial or ethnic origin, cultural background or culturally sensitive issues, disclosure of interests, political affiliations, curricula vitae, current employment and employment history, education/training qualifications, professional registration and affiliations, union membership, research grant and research publication history.

An important feature of the information collected by NHMRC is that, unlike many personal information databases compiled and used by various Commonwealth agencies, the information it collects as part of the grants process is provided voluntarily. In addition the database may, in respect of some individuals, include more personal information about them than was necessarily required. The fact that the personal information was provided voluntarily or that some of it may be 'excess to requirements' does not excuse the NHMRC from dealing with all of it in accordance with the APPs.

Context: RGMS

The current research grant management system used by NHMRC is RGMS ('Research Grants Management System'). It was implemented in 2009. A PIA was not conducted prior to its implementation, but this is not surprising. It was implemented at a time when PIAs were rarely conducted by Commonwealth agencies. In 2017 however, the OAIC issued the Privacy (Australian Government Agencies – Governance) APP Code 2017, which became effective on 1 July 2018 and now obliges agencies to undertake a PIA when implementing a significant project.

The existing grants management procedure is highly resource intensive for NHMRC – especially the front end grants approval process – for two main reasons.

First, because there are always more applicants than funds available, so there is a need to scrutinise each application closely to ensure best value for each research dollar is being achieved by the Commonwealth, and in satisfaction of current research priorities.

This requires the bringing together for each application of persons who are considered to be acknowledged experts in the particular field to which the application relates.

Secondly, NHMRC is bound by ordinary rules of procedural fairness and probity that apply to all Commonwealth agencies, and so principles of procedural fairness are applied – and need to be demonstrated to have been applied - in the consideration of each application. In particular, it is important that COI issues involving assessors be identified and managed properly.

Because NHMRC is the largest funder of health and medical research in Australia, there is significant professional and public scrutiny of its funding activities and the decisions that it makes. This means there is increased pressure on the NHMRC to ensure that each application for research funding is considered by a credible panel of experts, and that it is considered fairly. Equally, it is important that NHMRC be in a position to demonstrate that this was the case for each application.

Although RGMS currently does, and Sapphire will also, handle the subsequent management of grants over a number of years, it is fair to say that it is the early stages of the grants management system (i.e. the applications) as applied by RGMS/Sapphire that first raise the privacy issues to be considered in this PIA.

This is because, although funds are awarded to AIs, the reality is that in making funding decisions, the information provided or held about the backgrounds and research experience of the individual members of the team, described as 'Specified Personnel'- (and in particular the lead researcher (Chief Investigator) -is an important element of the decision making process. As already mentioned, much of this is personal information, and some of it is sensitive information.

In parallel, personal (including sensitive) information held by NHMRC is used in determining the appointment of potential members of panels and those who can act as assessors – partly to assist in determining whether they have the background expertise to assess a particular application, and partly to assist in determining whether they may have a COI which may prevent them from being involved in the assessment process.

The grants management process – in more detail.

Most of the basic decision making steps incorporated into RGMS will be replicated in Sapphire, and below is a brief analysis of the early phases of the grants management process, which are generally common between RGMS and Sapphire:

The grant management system is the end-to-end research funding process for the NHMRC. The process for this funding starts with the researcher accessing the grant management system, RGMS [soon to be Sapphire]:

- Researchers create a digital presence by applying for (currently) an RGMS account and populating their cv and profile (name, age and other personal details). This can be updated at any time by the researcher. Once this has been established, researchers can be included in grant applications and if so, the application Chief Investigator A (CIA) certifies to NHMRC that the application information (including any cv and profile data) in the application is accurate and correct. The RAO of an AI certifies the application on behalf of the AI and submits the application to the NHMRC.
- Applications are checked against eligibility criteria developed for the particular grant program by NHMRC staff. RAOs are notified if an application is not eligible.
- Staff assign the eligible applications to review panels,
    - To identify potential panel members and establish a review panel, NHMRC staff access RGMS and (1) identify those researchers who have self-nominated and (2) undertake a research key word search on researcher cv and profile information. In comparison, when implemented, Sapphire will use text analytics to identify potential panel members for review panels.
- Review panel members are initially only given access (through RGMS/Sapphire) to the Application Summary document (a small document which describes the application team, affiliated institutions, synopsis and research classification data).
- At this stage review panel members must declare any COI (not otherwise already identified by NHMRC staff) and if there is none, they will have access to the full application.
- Spokespersons are assigned to each application based on specific panel member expertise.

- Each spokesperson reviews the application and enters scores (and/or comments) into RGMS/Sapphire.
- For each application an assessor report containing assessment comments (deidentified) is, for some funding schemes, provided (via RGMS) to the applicant for the opportunity to comment (referred to as a rebuttal). The rebuttal is taken into account in any reassessment of scores. [Note the rebuttal process is being/has been phased out].
- Using the scores (following reassessment) applications are ranked with a set %, (some applications are designated *not for further consideration* (NFFC) by the full members of the review panel).
- Panel members are provided an opportunity to 'rescue' NFFCed applications.
- For consideration, applications are provided to all panel members for review and scoring in RGMS/Sapphire. At the end of the review panel process, any printed material is required to be destroyed, and members are directed to delete any applications and related material that may be held on their personal IT system.
- NHMRC Staff collate scores and draft funding recommendations for consideration by Research Committee and Council.
- Research Committee and Council do not see any personal information, only aggregated and non-identifiable information on the outcomes across priority areas and other measures plus the recommended funding dollars per application.
- The Minister for Health, who makes the final decision on funding under the NHMRC Act, is provided with the ranked application titles and the allocated grant number, the names of the researchers, the relevant AIs and the recommended grant funding dollars. The Minister is also provided with other information necessary to satisfy the requirements of part 4.2 of the Commonwealth Grants Rules and Guidelines.

Context: Sapphire

'Supporting Research Excellence'

Sapphire will replace the current Research Grants Management System (RGMS) which is due to cease in late 2019. As part of the implementation process, a small pilot grant opportunity will first be run.

The time frame for implementation of Sapphire (noting the small pilot project to be undertaken beforehand) is by the second calendar quarter of 2019.

Sapphire will be introduced progressively as the default system for new funding rounds; RGMS will not disappear immediately upon the implementation of Sapphire, but will exist side by side for some time in relation to funding programs that are currently being managed through RGMS. Eventually, however, it will disappear completely.

Sapphire will have significantly more functionality over RGMS in terms of its analytics capability. It will benefit assigners and assessors by offering tools to significantly streamline and simplify the matching of applications and assessors and outcome reporting.

To further reduce the burden on the research community, Sapphire is intended to:

- Be easy to navigate;
- Provide detailed onscreen help;
- Contain robust data validation;
- Provide visual cues to missing or invalid data; and
- Present the minimum number of questions to complete applications.

As previously stated, RGMS already contains a significant amount of personal information, as well as other research related information. Most of the personal information that it holds about individuals is held via their cvs. It is estimated that some 36,000 cvs will be migrated across to Sapphire as part of its implementation.

Although we understand Sapphire is anticipated to significantly reduce the time taken to undertake some of the key functions in the granting process (particularly the allocating of assessors) the basic steps required for the grants framework under RGMS will be undertaken in Sapphire as well.

Sapphire comprises two main components which are linked - OmniGrants and the Grants Management Accelerator (GMA). OmniGrants provides the grant program configuration, application submission and grant management capabilities through its forms and workflow engine, whereas GMA through its Semantic analytics engine provides the application assignment and assessment capabilities as well as the ability to enable outcome reporting.

1. **OmniGrants**

As described above, OmniGrants provides the grant program configuration, application submission, grant management and reporting capabilities through its forms and workflow engine. It is also the interim identity provider. In short:

It facilitates applications for funding by:

- Applicants with edit access to an application can name co-applicants on multi-author applications.
- The application owner controls view and edit access to the application form.
- Personal Information of all named Chief Investigators is extracted from their GMA Researcher Profiles through the use of OmniGrant application form Preview functionality.
- Application form based eligibility is checked by the solution at the time of Application submission to RAO to ensure compliance and satisfying of eligibility criteria.

Institution Application submission:

- AIs through RAO certify the veracity of the application, RAO's have access to the Application and Profile Reports to conduct this review.

- RAOs via the RAO Dashboard monitor Minimum Data and Application submission processes for their institution.
- The workflow engine can be configured to include any additional submission steps that may be required for a particular funding program.

Following approval of a grant, the grant management capabilities include:

- AIs receive and process offers of Award for successful applications via OmniGrant Approvals.
- OmniGrant workflow engine processes accepted offers and creates a Grant with payment tasks.
- Payment tasks can be paused/made payable based on the status of conditions or milestones imposed upon the release of funds.
- Forms support grant management processes such as Variation requests.
- Financial/contract management including acquittals.
- Eligibility checking during application phase.

Interim Identify Provider

- New User Accounts will be managed by OmniGrant in the interim, with a proposal to engage a completely independent identity provider service.
- Website form will collect basic personal information for the purpose of account creation.
- Message from user account creation web form to Omni will push details to create a user account in both OmniGrants and GMA.
- Role based user access model – both systems will apply the default security rights to the new user.

2. **GMA**

Through its Semantic analytics engine, GMA provides the researchers profile, grant program configuration, application assignment and assessment capabilities as well as the ability to enable outcome reporting. The key elements of GMA are:

The Researcher profile

- Provide Sapphire users with a single Profile, the ability to provide personal and research specific information for use by GMA's analytic engine and application processes.
- GMA analytic engine will use Research Profile data to classify an individual's area of expertise for use in assessment processes.
- Public Profiles - It is noted that, in the future, researchers may have self-selected elements of their cvs accessible through Sapphire as public profiles. Such a facility will not be a feature of Sapphire as initially implemented though.

- For the Pilot, the named user will have view and edit access to their Researcher Profile. NHMRC users will have view access. Sapphire Administrators will have edit access.
- Researchers will be able to indicate if they want their RAO to have edit access to their Researcher Profile.
- Researchers will be able to integrate their Sapphire Profile with their ORCID account, making data import fast and simple.
- Applications submitted to NHMRC will be made available in GMA to be assigned to review panels based on applicant defined peer review areas.
- GMA analytic engine will use application data to classify an application to ensure assist in targeting it to be most appropriate assessors.
- Application assignment processes include identifying and securing ideal panel membership, requesting COI (and suitability to assess survey) and final allocation of applications to assessors.
- Importantly, the finalisation of Application assignment processes will be conducted by NHMRC staff.
- Access to view panels and applications is controlled by role and application level permissions. GMA program configuration will allow NHMRC to control what information is made available to active panel members and at what time.

With respect to what aspects of a researcher's (data) profile are used within the various GMA algorithms, we were advised of the following categories, some of which contain personal/sensitive information:

Algorithm	Description	Profile Data Used
Member splitting	Relies on the parts that we are balancing which are State, Title, Gender and Institution	Gender Title Primary Institution
Application Split, Spokesperson Assignment and Assessor Selection	Uses COI and suitability that was filled out by the panel members.	None
External Assessor Selection	Uses the same data as from the ranked candidate search	Names Title Gender Research Keywords Peer Review Areas Fields of Research PhD Awarded Year Primary Institution
Auto COI	Uses historic applications, publications and work history from the user profiles	Publications Employment History
Auto Suitability	Uses profile keywords	Research Keywords
Ranked candidate search	Uses Profile keywords, PhD year, etc. (everything shown on the dialogue)	Names Title Gender Research Keywords Peer Review Areas Fields of Research PhD Awarded Year Primary Institution

Subject Classification	Uses historic application text to create the subject classifiers (not using profile information directly).	None

Discussion

Although Sapphire is clearly a highly sophisticated IT system, from a privacy perspective it does not appear that, in its implementation and early stages at least, it will be collecting, using or disclosing information that is not already being collected, used or disclosed under the current RGMS system.

Accordingly, most of the privacy issues relate to the existing procedures as well as Sapphire.

Three features of the NHMRC's existing grants management procedures, which will [*broadly at least*] be replicated in Sapphire, have contributed in particular to the privacy issues surrounding the implementation of Sapphire. They are:

- NHMRC has only limited control over what unsolicited personal information (particularly sensitive information) may be provided voluntarily by researchers (or via their RAOs – see below);
- The feature of third parties being given consent to access and amend an individual's personal information held by the NHMRC ; and
- Researchers giving consent for their personal information to be provided to overseas recipients for various reasons (e.g. if an expert assessor resides overseas or there is an opportunity for gap funding or co-funding to be provided by another institution) at a time when in some circumstances it is likely/possible the individual or even the NHMRC may not necessarily even know which particular country the information may be sent to at the time it is collected.

We note that all three of these aspects are regarded by NHMRC staff as fundamentally necessary features of the grants process, so on balance they must be managed rather than eliminated.

There is a strong incentive for applicants to provide as much personal information as they can to maximise their chances of grant applications being successful. Equally, members of the research community and other health/research professionals are usually keen to be considered for appointment to panels – partly because the NHMRC Funding Agreement (clause 23) requires an AI to make available to the NHMRC, free of charge, Specified Personnel to provide input into the peer review process and, as noted previously, partly because appointment does provide an element of recognition of their status in the research community.

Some of the personal/sensitive information collected by NHMRC is collected for very specific reasons.

As noted previously, the cv of an applicant is an important element in the assessment process, and any unexplained gaps in an applicant's career may garner attention in the assessment process. As part of the cv process, applicants are invited to provide information that may explain career interruptions of a certain type – e.g. carer responsibilities or child rearing. This is a positive element of the cv process, but these types of information may amount to sensitive information and need to be treated accordingly by NHMRC.

Sapphire clearly represents a significant technological step forward in the handling of the grants management process for NHMRC. Based on our understanding of Sapphire and the agency's grants process, we formed the view that the Privacy risk areas inherent in Sapphire - as it will be applied at implementation - were to be found in respect of satisfying the following APPs:

- Openness and Transparency about how the personal information is managed [APP1]
- The storage and security of the information - including access to the information by NHMRC staff and contractors [APP 12]
- The cross border disclosure of sensitive information [APP 8]
- The obligation of NHMRC to maintain the accuracy of the personal information the agency holds [APP 10]
- The use of the information for purposes beyond the purpose of its original collection [APP 6]
- The migration of existing personal information from RGMS into Sapphire, raising risks of information quality being affected [APP10]

Although this project involved assessment against all the APPs, the above are the key risk areas which we focussed on in the development of this PIA.

Legislative Framework

We regard the provisions of the NHMRC Act as technology neutral in respect of any requirements regarding the grants process. NHMRC has promulgated RGMS (and Sapphire in the future) as the only technology portal through which grant applications will be accepted by it.

Our understanding of Sapphire has led us to form the view that NHMRC's existing legislative underpinning for the collection, storage, analysing, use and disclosure of personal information (particularly, in this context, sensitive information) does not require further strengthening to support the implementation of Sapphire in its currently proposed form.

So, the simple fact of adopting a more sophisticated and powerful internal collection and analysis system which involves the migration of an existing database within the agency's own structure should not automatically make any difference from a legal perspective – particularly when it appears the information provided historically will, initially at least, continue to be used only for the primary purposes for which it was originally collected, or for a reasonably expected secondary purpose [APP 6]. A different answer may be required in the future if analytics tools are developed within Sapphire which contemplate the use of personal/sensitive information in other ways beyond the original, relatively narrow purposes of grants management.

ANALYSIS OF COMPLIANCE WITH THE APPs

APP1 – Open and Transparent Management of Personal Information

This APP requires that an agency must:

1.2 Take reasonable steps to implement practices, procedures and systems that:

- *Ensure the entity complies with [the APPs]; and*
- *Enables the entity to deal with enquiries or complaints about compliance;*

1.3 Have a clear and up to date policy about how it manages personal information;

1.4 The policy must specifically contain the seven specific pieces of information identified in APP 1.4;

1.5 Take reasonable steps to make its privacy policy available free of charge in an appropriate form (usually on its website); [and]
1.6 Take reasonable steps to give a person a copy of its privacy policy in the form requested.

Analysis

NHMRC has recently revised its Privacy Policy, which is available on the agency's website. This policy is regularly reviewed, in accordance with APP1. Clause 17 of the Australian Government Agencies Privacy Code, issued by the OAIC, requires an agency to regularly assess the adequacy of its privacy practices, procedures and systems (including its privacy policy and collection notices) to ensure their adequacy for the purpose of compliance with the APPs and their general currency.

We assessed the Privacy Policy against the requirements of APP 1 and are satisfied that it meets all those requirements – see below for a breakdown of our analysis.

More particularly, we reached the view that the core elements of the NHMRC's Privacy Policy do not appear to require any modification in order to support the implementation of Sapphire.

APP 1.2 The NHMRC has a Privacy Management Plan, the most recent version of which is dated 1 July 2018, which we understand was developed using the guidance in the OAIC Privacy Management Framework.

The NHMRC's Privacy function sits within the Strategic Projects and Support Section in the Research Quality and Priorities Branch. It is responsible for ensuring that the agency complies with the Privacy Act, by:

- Ensuring the provision of privacy management training to staff;;
- Assisting business areas to understand the practical application of the Privacy Act;
- Coordinating a register of PIAs;
- Having responsibility for the privacy policy and privacy information published by the agency;
- Assisting business areas to respond to privacy breaches; and
- Managing the NHMRC's relationship with OAIC.

With the implementation of the OAIC's Australian Government Agencies Privacy Code on 1 July 2018, there was some re-arrangement of privacy functions, primarily as a result of the required appointment by the NHMRC of a Privacy Officer(APS) and a Privacy Champion (SES), the latter of whom is the Senior Responsible Person with prescribed responsibility for these functions.

We are satisfied the NHMRC does have an ability to deal with inquiries or complaints from individuals about the entity's compliance with the APPs. In particular, the privacy policy sets out how an individual can contact the privacy officer to complain that the NHMRC may have breached any of the APPS – providing the options of contact by telephone, email or written mail.

APP 1.3: As noted above, the NHMRC has recently adopted and issued a new privacy policy. Subject to our comment below about the reasons for collecting personal information (APP 1.3), the Privacy Policy provides a good general overview of how the agency manages personal information.

NHMRC collects and uses large amounts of personal information for many of its non-granting activities, including its roles under the RIHE Act and PHCR Act, participating in voluntary targeted consultations, receiving complaints about research misconduct or fraud, employment applications, and appointments to committees or working committees. Accordingly, the Privacy Policy contains an extensive list of ways in which NHMRC may collect personal information, what those categories of personal information are, and for what purpose they are collected.

Relevantly for the role of Sapphire, the policy sets out the reasons for collecting personal information and the kinds of personal information collected for grants purposes as being simply:

- Participating in grant review processes (including as an assigner or assessor);

In view of the fact that grants funding and management is the core role of NHMRC, and the collection of personal information is an important aspect of the process, this is a relatively brief description of the primary reason for collecting the information. We recommend that, when an opportunity arises to review the Privacy Policy, a more expansive description of the reasons be inserted in the policy.

APP 1.4(a) to (g): We assessed the contents of the policy against the seven specific information requirements: and are satisfied the Privacy Policy includes the information required by APP 1.4(a) to (g).
See below for our individual comments in respect of each paragraph's requirements.

APP1.4(a) – kinds of personal information held: Some of the categories of personal information that may be held about an individual (e.g. driver's licence number, number of dependants), and the purposes for which they are held by NHMRC, are not relevant to Sapphire. But the following entries in the Policy are specified for the purposes of APP 1.4(a) and will in particular circumstances be relevant:

> Sex/gender, physical or mental health, disability status, racial or ethnic origin, cultural background or culturally sensitive issues, disclosure of interests, political affiliations, curricula vitae, current employment and employment history, education/training qualifications, professional registration and affiliations, union membership, research grant and research publication history.

We could not think of any other category of personal information collected by NHMRC relevant for Sapphire that was not set out in the Privacy Policy.

APP1.4(b) – how personal information is collected and held:
The Policy states that 'the main way in which NHMRC collects personal information is when you provide it' (p. 5). It notes that the NHMRC may also collect personal information via a third party when an institution makes various types of application to the NHMRC (p. 5). The most obvious category here would be the lodging of an application for a grant by an AI, containing personal information relating to its proposed research team ('specified personnel').

The personal information collected for grants management purposes is provided electronically, through the completion of online forms. Although new online forms are being developed to support the implementation of Sapphire, the basic arrangements will not change in any significant way. We note with approval that all

forms are being reviewed as part of the process for the implementation of Sapphire, in order to ensure that only personal information necessary for an application will be collected.

Because Sapphire is essentially a far more powerful and efficient internal storing, matching and analysing IT system used by NHMRC staff, the external differences that individuals (particularly researchers) will notice after its implementation in relation to the collection and use of their personal information are minimal if at all.

With respect to the requirement in the second limb of APP1.4(b), i.e., stating how personal information is held, the Privacy Policy contains a section titled 'Storage and Security of Personal information'. It adequately outlines the steps that NHMRC takes to protect the security of personal information it holds by reference to storage in accordance with the requirements of the PSPF and the Australian Signals Directorate Information Security Manual, and management in accordance with the requirements of the *Archives Act 1983*.

APP 1.4(c) purposes for which personal information is collected, held, used and disclosed

The Privacy Policy does not have a specific area where it sets out in detail the vast number of (proper) purposes and uses that it makes of the personal information that it collects; however in describing the kinds of information that it collects, it does effectively explain those purposes - e.g. in responding to participating in a grant review process ('Collection of Your Personal Information' - p.5) . See also the section titled 'Use or Disclosure of Your Personal Information' (p. 10), which, despite its title, is in effect more a statement of circumstances where the NHMRC will not be taken to have breached its privacy obligations in respect of personal information. It is, however, a useful compiled list of relevant circumstances.

APP 1.4(d) – how an individual may have access to their personal information and seek its correction

This requirement is adequately addressed on page 15 of the Privacy Policy.

APP 1.4(e) – how to Complain

This requirement is adequately addressed on page 16 of the Privacy Policy.

APP1.4(f) – circumstances of Disclosure to Overseas Recipients

The Privacy Policy outlines three primary circumstances where personal information may be disclosed to overseas recipients by NHMRC(page 11). They are:

- Where personal information (contained in an application) must be sent overseas to an expert reviewer or assessor as part of the review process;
- Disclosure within jointly administered research funding schemes involving overseas researchers or funders
- Disclosure to support international cooperation in fostering global health and medical research goals – primarily regarding local researchers with expertise in particular areas.

It includes links to a site that provides more comprehensive information about international research activities.

The Privacy Policy also states at page 11:

NHMRC will prompt applicants with a notice that seeks their express consent to overseas disclosure at the time of making their application. Applicants can elect not to have their information sent overseas.

It is a minor point but arguably, in respect of the first dot point circumstances outlined above, it is wrong to say personal information must be sent overseas – suggesting a degree of compulsion or contractual obligation. Where a project is jointly funded with an overseas body, then clearly it would reasonably be expected that NHMRC would have to send personal information overseas, because the overseas party is an integral part of the assessment and funding process. However, where the reason for sending it overseas is because a view has developed that the best/most appropriate person to assess the application resides overseas, that is a subjective test and suggests that if that person is not available, then by definition the application must fail. We assume that in practice, if the 'best' person were not available, then alternate arrangements would be made and someone locally would be identified. Accordingly, we recommend that the wording in the policy be amended at an appropriate time 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.

APP 1.4(g) – if there is a likelihood of disclosure of personal information to overseas recipients, those likely countries - if practicable

The Privacy Policy does not contain a list of likely countries, but does explain, as set out above, the likely circumstances in which personal information may be sent overseas. It also provides a link to a site that contains information about international research activities and countries are specified on that site.

APP2 – Anonymity and Pseudonymity

This APP requires that individuals must have the option of not identifying themselves, or using a pseudonym in the collection of their information, unless:

- *The agency is required or authorised by law to deal with identified individuals; or*
- *It is impracticable for the agency to deal with people who have not identified themselves.*

Analysis

The Privacy Policy contains the statement 'In the case of applications for research grants, it is not practicable for NHMRC to deal with you on an anonymous or pseudonymous basis. NHMRC will not accept a grant application or report that is anonymous or not in your real name.' (page 9 of Privacy Policy).

As previously noted, a key element of the current grants application process is the collection and use of significant amounts of personal/sensitive information about identified individuals for the purpose of assessing those applications.

The nature of the grants process means that the identities of the individuals who are part of the research application are critical to determining grants. It is impracticable, if not impossible, for NHMRC to deal with grant applications that would rely in great part upon the apparent expertise and achievements of non-identified people.

Equally, it is impracticable for NHMRC to appoint assessors who are not identifiable. A major factor in the appointment of assessors to panels is the determination whether there are potential conflicts of interest

raised in respect of an individual, and it would be impossible to undertake a conflict check involving a de-identified individual.

There would not appear to be any changes to the Privacy Policy, or other administrative changes, that need to be made in respect of the implementation of Sapphire in order to meet the requirements of APP2.
Nor could we see any changes that needed to be made to the Sapphire framework to address this APP.

APP3 –Collection of Solicited Personal Information

3.1 An agency may only collect personal information (other than sensitive information) that is reasonably necessary for, or directly related to, the agency's functions or activities.
3.3 [Sensitive information] An agency may only collect sensitive information:

- *With the individual's consent and the information is reasonably necessary for, or directly related to, one or more of the agency's functions or activities; or*
- *where one of the exceptions in APP 3.4 applies.*

3.4 [Exceptions clause –none of which appear to apply in the current circumstances being considered in this PIA]
3.5 An agency must collect personal information only by lawful and fair means.
3.6 An agency must collect personal information about an individual only from the individual unless:
(a) the individual consents to the collection of the information from someone other than the individual: or
(b) it is unreasonable or impracticable to do so.

Analysis

As the NHMRC frequently emphasises in its publications, the personal information that it collects about individuals is overwhelmingly provided by those individuals with consent and, in particular, the information provided by individuals (principally researchers) for research funding purposes is only accepted by NHMRC if the individual has confirmed their consent to its use and disclosure on the online form.

There is in fact one proposed feature of Sapphire which, from a privacy perspective, is an improvement over the existing RGMS. When an individual researcher is added to an application, an email will be automatically generated to the individual by the system, asking them whether they consent to be added to the application.

With respect to whether the information is reasonably necessary for, or directly related to, the NHMRC's functions or activities – the categories of personal information generally required to be provided would all appear to be the kinds of information that a research funding institution (whether private or government) would reasonably be expected to collect in order to properly address a funding application or when appointing an assessor of an application. In particular, for example, this would cover cvs, professional memberships, publications, etc.

All applying researchers must have a 'My Profile' cv held electronically by NHMRC. It is meant to be/required to be kept up to date by them or their RAO and used for research funding and assessor appointment activities. Some individuals who have retired from research but who are willing to be appointed as assessors from time

to time for particular projects may continue to retain a 'My Profile' cv with NHMRC. These are all held on RGMS/Sapphire.

With particular respect to the collection of sensitive information such as ethnicity and gender for the general categories of grants managed by NHMRC, these pieces of information would not ordinarily be collected, but they are collected by NHMRC in the context of programs aimed at encouraging indigenous researchers and addressing current gender inequality in research funding and this is made clear to potential applicants.

With respect to the collection of sensitive information about health issues – these are only collected in the context of a researcher being offered the opportunity to outline career breaks in their cv in order that potentially adverse conclusions might not be otherwise unfairly drawn about their track record and abilities.

In all three sets of circumstances outlined above, the individual must specifically confirm that they are providing the information voluntarily.

In relation to APP3.6 - as outlined earlier, RGMS/Sapphire requires an RAO from an AI to certify/verify any personal information contained in an application (as well as all the other contents of the application). Whether this amounts to the collection by the NHMRC of personal information 'from someone other than the individual' is a moot point, but probably also academic. By definition a researcher must have consented to their cv/profile being part of an application which is lodged by an AI anyway.

The proposed standard online application form for Sapphire includes, in the Privacy Section, an entry titled '*Access to your profile*". It contains the statement :

> By default, your primary institution's Research Administration Office has view access to your profile. You may also allow the RAO to edit your profile.

There is provision for the individual to select an AI, and then an option (Yes/No) to select whether the relevant RAO has been authorised by them to also have what is termed 'RAO edit access'.

We note that the specifications documentation for Sapphire states that:

> A feature of Sapphire [GMA] will be that Researchers will be able to indicate if they want their RAO to have edit access to their researcher profile.

Although the relevant parts of the application forms seeking particular sensitive information with respect to gender and indigeneity purport to be voluntary, we inquired whether a failure to 'tick' one of the boxes in this space could prevent an applicant from proceeding further with their application, or lead to the rejection of their form as incomplete. We are satisfied that the questions are stand alone, except where a person seeks to take the benefit of a grants policy that is aimed at achieving gender neutrality or in assisting indigenous applicants – in which cases it is appropriate for an applicant to indicate their gender or indigeneity.

APP4 – Dealing with Unsolicited Personal information

If an agency receives unsolicited information, it must decide whether it could have collected it under APP 3.

Analysis

OAIC considers that unsolicited information includes information provided to an agency that is additional to the information that the agency requested (OAIC APP *guidelines*, para 4.8).

The implementation of Sapphire does not contemplate the collection of unsolicited personal information nor, as far as we can ascertain, does it increase the likelihood in any way that unsolicited information would be solicited or collected.

NHMRC's privacy policy specifically addresses the question of the receipt of unsolicited personal information.

Although the cv forms are prescriptive of what information is/can be required – 'structured information'- the cv forms do contain free text boxes where an individual may provide personal information outside what is required or expected by the application process.

Although the information required by NHMRC is specified in the relevant forms, there is a natural and understandable inclination for applicants and potential assessors to provide personal information that goes beyond what the forms may require, out of a desire to maximise their opportunities for success in the awarding of a grant or the appointment as an assessor.

The advice and instructions issued to potential applicants for the various forms of grants do attempt to minimise the risk of collecting unsolicited/unnecessary personal information – e.g., under the heading 'CV Requirements', the current instructions for the 2018 round of NHMRC Partnership Projects contain the statement:

> For Partnership Projects, you are only required to complete those sections outlined below. Should you enter more information than is required, only the required information will be imported into your application…..Instructions for entering CV information in RGMS are provided in the RGMS User Guide – Introduction to RGMS on the NHMRC website.

There will be practical limits to the risk of collection of unsolicited personal information under Sapphire through the use of character limited free text boxes and dropdown list options only. Also, as noted earlier, the implementation of Sapphire has involved a review of all information categories to limit them to only the information that is necessary to support an application.

APP5 – Notification of the Collection of Personal Information

An agency that collects personal information about an individual must (at or before the time it collects the information or, if not practicable, as soon as practicable) take such steps as are reasonable in the circumstances to ensure the individual is aware (e.g. by giving them notice) of the following:

- *agency identity;*
- *details of any law that requires or authorises the collection;*
- *the purposes of collection;*
- *consequences if the information is not collected;*
- *the entities that the agency usually discloses that kind of personal information to;*
- *information about the agency's privacy policy;*

- *whether the agency is likely to disclose the information to overseas recipients [including the names of those countries if practicable].*

This must be done before or when it collects the information or, if that is not practicable, as soon as possible after collection.

Analysis

With respect to the consequences of not collecting the required personal information, it is clearly outlined that the failure to provide the required information will or may lead to the application being rejected as not meeting the applicable eligibility criteria.

The proposed grant application form [based on the draft screen shot for Sapphire provided by the implementation team] clearly refers applicants to NHMRC's privacy obligations, refers them to its Privacy Policy, and urges applicants to read and understand it before completing their application.

With respect to the likelihood of disclosing information to overseas recipients, it is noted that the Privacy Policy addresses the circumstances where this may occur and, in any event, it is also canvassed more particularly in the information notes provided for any particular grant program.

APP6 – Use or Disclosure of Personal Information

An agency must only use or disclose personal information for the purpose for which it collected it (the primary purpose), and not for another purpose (the secondary purpose) unless:

- *the person consents; or*
- *an exception applies.*

The relevant exceptions here are that:

- the person would reasonably expect the agency to use or disclose the information for the secondary purpose, and in the case of sensitive information, the secondary purpose must be directly related to the primary purpose [APP 6.2(a); or
- the use or disclosure is required or authorised by law [APP 6.2(b)];

The implementation of Sapphire does not currently involve any changes to the Agency's external business that would impact on the application of the current exceptions that already apply in respect of APP 6.

Apart from when an individual completes an application form in respect of a co - funded project, they properly believe they are applying for funding from the NHMRC. However, as noted previously, NHMRC does seek, from time to time, to assist an applicant whose research project has been recommended for funding, but is not funded, by bringing the application to the attention of a third party funder. This would involve the forwarding of the application information, assessment information (including individuals' sensitive information – if any), to a third party.

There is a privacy issue under APP 6 in this process, in that the primary purpose of the typical class of application would be to receive NHMRC funding. In our opinion, however, to forward the information to a

third party for further funding consideration would be regarded as a secondary purpose. APP6 does provide an exception where the individual consents and, in the case of sensitive information, the secondary purpose must be directly related to the primary purpose [APP 6.2(a)].

We note in this context that the Privacy Policy states, under 'Use or Disclosure of Your Personal Information', that 'NHMRC will not be taken to have breached its obligations under this policy or the Privacy Act where a grant applicant has explicitly indicated, or made NHMRC generally aware, of a wish for the application to be considered by other funding bodies and research institutions, such as co-funding organisations or the applicant's own institution.'

We also note that the draft online application form developed for Sapphire contains the following notification/entry:

> **Gap consent** (*with a link to an explanation of what gap funding is)*
> Do you give consent for NHMRC to provide this application, snapshot reports and information about the results of NHMRC's assessment of this application to co-funding organisations (gap funders)?
>
> **Yes No**

We are of the view that, in respect of any sensitive information contained in an application (primarily in a cv), the ticking of the 'yes' box would amount to consent for the disclosure of their personal information for the secondary purpose of consideration by another funding organisation – which can reasonably be seen as being directly related to the primary purpose of funding being (otherwise) provided by NHMRC.

APP7 – Direct Marketing

This APP restricts an agency from using or disclosing personal information for direct marketing purposes.

Analysis – There is no direct marketing engaged in by NHMRC.

Not applicable

APP8 – Cross-Border Disclosure of Personal Information

Before an agency discloses personal information to an overseas recipient, the agency must take such steps as are reasonable in the circumstances to ensure the overseas recipient does not breach APPs 2-13 in relation to the information.

The two key requirements set out in APP 8 are:

- *Before it discloses the information, the NHMRC must reasonably believe the overseas recipient is subject to a law or scheme that is substantially similar to the APPs and the individual has access to privacy appeal rights in that overseas place[APP 8.2(a)]; or*

- *Otherwise, that the NHMRC expressly informs the individual that if they consent to the disclosure of the information, the above obligation does not apply and, after being so informed, the individual consents to the disclosure. [APP 8.2(b)].*

Analysis

From time to time, NHMRC sends limited categories of personal information collected in RGMS overseas (and proposes to continue to do so following the implementation of Sapphire).

Part 9.5 of the NHMRC's Funding Rules 2018 state 'For some funding schemes, NHMRC may disclose your personal information to an overseas based co-funding organisation. NHMRC may also appoint peer reviewers from overseas countries, where there is a need, and in accordance with the Privacy Act and NHMRC's Privacy Policy. RGMS will prompt you with a notice that seeks your consent to overseas disclosure.'

The NHMRC's Privacy Policy specifically addresses the issue of disclosure of personal information to overseas recipients at pp. 11-12.

The Policy addresses the following three scenarios:

- Disclosure as part of the peer review/assessor process - on the basis that the most qualified researcher for assessing any particular application may be overseas. – 'NHMRC will prompt applicants with a notice that seeks their express consent to overseas disclosure at the time of making their application. Applicants can elect not to have their information sent overseas for review.'
- Disclosure within jointly administered research schemes – Funding schemes to provide assistance to Australian researchers to participate in collaborative research projects with international researchers. A link is provided for information about those funding schemes .Disclosure would be made generally for the purposes of review of applications. 'Applicants are advised of this possibility at the time of making their application'.
- Disclosure to support international cooperation – in order to foster global health and medical research goals, NHMRC and its equivalent overseas organisations will from time to time share personal information about researchers with expertise in particular areas. A link is provided for information regarding those organisations and countries.

The currently proposed APP 8 statement for Sapphire on the application form is as follows:

> 'In addition, and in accordance with Australian Privacy Principle 8 in the Privacy Act 1988 (Cth), we seek your consent to send your personal information (constituting 'Assessor Snapshot Report') overseas, for the purposes of peer –review of this application if required. NHMRC uses the expertise of some peer assessors who[reside] overseas. While we take every effort to protect your personal information, assessors outside Australia are bound by their own country's laws and consequently [we cannot] provide assurance that your information will be handled in accordance with the same standards as required by the Privacy Act 1988 or that you would have[….]remedies should your personal information be released in breach of local privacy laws..'

The proposed prompt does not refer to the possibility of personal information being sent overseas for co-funding purposes, only peer review purposes. However, this is a general form. It is likely that any material

supplied in relation to a particular co-funded grant scheme would also include a 'consent box' relating to the particular co-funding country (see below). Alliances with overseas co-funders are usually well identified in the relevant funding papers.

We do have a concern whether the form of consent to be provided is fair at the time it is provided in view of the fact that the applicant will in many cases not know which country the information would likely be sent to at the time of giving the general consent.

Arguably, even if a general consent for overseas disclosure has been given at the commencement of an application process by an individual, if NHMRC does subsequently propose to disclose the information to an identified overseas recipient, the NHMRC staff should go back to the individual and confirm their consent in respect of the particular country once it is known.

It is noteworthy, for example, that RGMS/Sapphire does give an applicant the option of not having their application provided to any particular co funder/gap funder – see ' 2018 NHMRC Advice and Instructions to Applicants - Help Text in Sapphire to applicants (p. 7) - Option of declining to let a particular institution see your funding application' – but a similar option does not appear anywhere for declining to let an application be forwarded to a particular country.

We note that the Privacy Policy also states that, at the time of application, an applicant can elect not to have their information sent 'overseas', but with no provision for declining in respect of a particular country once the country may be identified or known. Sensitivities regarding particular countries, as opposed to 'overseas' more generally, does not appear to be accommodated.

In practice, the identity of overseas parties involved in some collaborative research or partnership projects will invariably be known and disclosed at the time the funding material – including the application form - is issued. A simple example is the Collaborative Research Grants Funding NHMRC-NIHR Program, involving the USA. In those kinds of programs, the consent would be adequate for the purposes of APP8. Where, however, the identity of an overseas recipient becomes clear only after an application is lodged (e.g. when the nature of the proposed research becomes clear and an assessment is made of where the potential best reviewers may reside – particularly where the pool of potential experts in that field of research is extremely small), then there is a question mark over whether a general consent at the time of lodging an application is a genuinely valid consent. There is a privacy question whether, once the agency has decided where to send the information, it should contact the applicant and advise them of the proposed country and seek their specific consent at that time.

Such a procedure would clearly satisfy the requirements of APP8, but we acknowledge that there is a question of whether it is a practical course of action for the NHMRC in light of the low risk of refusal and the potentially significant resource implications of doing so. We also acknowledge that a key platform of the assessment process is the anonymity of the assessors and, because of the relatively few experts in each area of medical and health research, disclosing the country where the information will be sent could be tantamount in some situations to effectively disclosing the identity of the assessor.

While acknowledging these risks and the inherent resource implications, we recommend that consideration be given to developing a policy of advising applicants of the specific country where their information may be sent, once it is known, but subject to considerations of anonymity, practicality and other factors.

APP9 – Adoption, Use or Disclosure of Government Related Identifiers

This APP prevents private sector organisations from using government related identifiers, such as TFNs or Medicare numbers .

Analysis

Not applicable to NHMRC, which is a government agency for the purposes of the Privacy Act (see section 6(1) Privacy Act).

APP10 – Quality of Personal Information

10.1 An agency must take reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete.
10.2 An agency must take reasonable steps to ensure that the personal information that it uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

Analysis

Three risk areas have been identified:

- Quality of information provided by individuals/RAOs in the first place;
- Risk of personal information corruption during the data migration process from RGMS to Sapphire;
- (Unauthorised) Amendment of personal information by RAOs.

Quality of Information Provided to NHMRC

Although most of the personal information provided to NHMRC in the course of the grants management process is provided in a structured way, there is provision for free text in application forms as well. It would be reasonable for NHMRC to assume that an individual researcher would provide accurate personal information about themselves, and there is in any event a filtering system provided by each AI's RAO, who must certify the accuracy of information contained in any particular application.

How up to date the personal information that it holds may be at any particular time is another issue.

It would be unreasonable to expect the NHMRC to actively review all personal information that it collects in RGMS/Sapphire on a structured or regular basis. The question is what steps, if any, should NHMRC be expected to take to ensure that it meets the 'reasonable steps' test in APP10 for accurate, up to date and complete personal information collected through Sapphire?

In our opinion, an annual circular email to all researchers on the NHMRC researchers database, urging them to review their cv/profile to make sure they are satisfied the information is up to date and accurate would be

a reasonable step. The email should, however, recommend that the individual personally review their cv/profile, and not just refer/delegate the role to their RAO (although NHMRC could not prevent any individual from doing so).

Data Migration from RGMS to Sapphire:

At a very basic level, and leaving aside the anticipated high matching performance of Sapphire itself, the success of Sapphire will depend upon there being no loss of quality during the migration of the data from RGMS during the Data Migration Phase.

A data migration strategy (dated 21 December 2017) was initially developed as part of the implementation of Sapphire, and the procedure for the migration of RGMS data is more particularly set out in a paper titled the Sapphire Data Migration Design Document, dated 26 January 2018. The Data Migration Strategy is based upon the assumption that data cleansing where possible will be performed in the legacy RGMS solution prior to migration (Data Migration Strategy and Approach, version 1.0, cl. 2.3)

Clause 15 of the Data Migration Strategy document addresses the question of a data migration audit. Currently, it is proposed that the firm of McGrath Nicholls will undertake an audit, although the specific terms or nature of the audit are still being discussed.

We have reviewed the procedure as set out in those documents. They represent the key design elements to extract, select, validate, transform, enrich and cleanse the RGMS data required for the Sapphire solution.

Data migration will take place in two phases – phase 1 is the critical phase with respect to the migration of data which may contain personal information and this is being undertaken by the firm Semantic Sciences. Phase 2 principally relates to the migration of grants data (although it appears there will be migration of some duplicated personal information as well) and this will be undertaken by a separate firm (F1 Solutions).

The principal point to note is that the data migration process - in relation to the migration of personal information at least - does not involve the actual manipulation of any of that data; subject to one point below, the process will involve not touching the source data; it is being directly lifted and copied across, which should mean the risk of corruption/error arising as a result of the migration process should be extremely low.

Although a formal audit will be undertaken of the data migration process, there is a quality assurance/data validation process being undertaken during the migration process as well. The firm Semantic Sciences is undertaking the loading of the files containing personal information, and they are conducting checks of the

information as it is copied . Extracts of any identified possible errors ('error logs') are sent to the NHMRC's Sapphire team for checking of the data. We understand that, to date, the errors identified have related to duplication of data only.

Six data migration groups have been classified in phase 1. The relevant groups /RGMS Data Entries for this PIA (*i.e. they include personal information*) are Master Lists (0100), Profiles (0300), Applications (0400) and Assessment (0500) . All four of those sets of data will be migrated into GMA, and some small duplicated elements of Master Lists and Institutions will also be migrated into OmniGrants.

Although in general the personal information will be copied and carried across in a seamless way, the opportunity is being taken to 'cleanse' some categories of information. For example, there are specified categories of 'excluded users' who will be excluded from migration – they are, essentially, filters to exclude inactive accounts (e.g. inactive for 5 years) or persons identified as 'permanently unavailable' - which we understand relates primarily to deceased or retired researchers.[p. 10]. These cleansing processes do, in theory, raise the risk that data might become inaccurate, although it appears the risk is low.

0100 Master Lists

This includes table 0109 conflicts of interest. Our understanding is that this table will not be changed in any way and will simply be transferred directly across to GMA. We note that 'a cut-down version of the profile extract including the key user account information will be provided to OmniGrants' as well 'to load and generate User ID's'.

0108 Field of Research

This is a research classification that applies to applications and researchers. All fields of research will be provided – i.e. there will be no touching of the source data in the migration.

Conflict of Interest (COI) (0109)

Historical COI will be used by GMA for future COI prediction. It is noted that the document states 'All fields in the conflict of interest view will be provided' – i.e. the data will not be varied or manipulated in any way prior to or during migration – 'There is no transformation required for this data entity'. The actual declarations of COI will be in 0500 Assessments.

Sapphire will 'flow' the following profile data across to OmniGrants: Member ID, title, First and Last Name, PHD and User Primary Institution Code.

0300 Profiles

This is a set of tables containing personal data about researchers.

Not all records will be migrated and where records are excluded the exclusion rules are set out in the document on p. 4 of the Sapphire Data Migration Design Document. None of those exclusion rules appear to relate to any personal information.

0300 Profiles – Profile CV.

This is one of the key areas that we focussed on.

The Design Document provides at p. 18 that all the contents of the profiles will be sourced from RGMS. Before migration, however, the data will be varied by deleting the following limited number of categories:

- The excluded users list (cl 2.1) – mainly confirmed inactive or test accounts;
- Cleansing of Superfluous characters (e.g. '?' and '??') from the research methods category Text regarding primary and alternate institutions – which was deemed to be a duplication of information.

The Design Document noted that, during the cleansing process, 29 entries failed to indicate the year their PhD was awarded. In order to facilitate the importing of these awards, they have all been allocated a notional date

of 1900. It is noted that a similar approach has been taken in at least three other areas - 'Community Engagement' , 'Relative to Opportunity' and 'Appointment'– where the cv may not have captured the relevant years (see pp. 24, 27 and 39). In those cases, blank start year fields have been completed with a value of 1900. It was also noted that, for 'Relative to Opportunity', GMA requires that a record's start year date is less than or equal to the end year date. A significant number of records were found to have violated this rule. Accordingly, the issue has been addressed by having the end year date set to the same value as the start year. Although these strategies have enabled the data migration process to proceed apace, at an appropriate time the correct dates for these awards should be entered into Sapphire for the sake of accuracy of the personal information record.

The Design Document provides that the vendor (Semantics) will complete the validation of the profile cvs.

0400 Applications
Application data is being provided to GMA to facilitate the algorithms classifying individuals by matching a team member with application content. Each application extract will contain basic application data which will include basic information about the team members (including their role) of an application.

0500 Assessment.
Assessment data is being provided to GMA to facilitate the algorithms in further classifying individuals. Each assessment extract will contain application ID, assessor level of suitability, assessor COI level and assessor role.

The Migration Design Document provides (p. 56) for a data reconciliation plan, which notes that the data received back from vendors' extracted files will be verified for completeness and correctness against data which was supplied to them as part of the data extraction process. 'The completeness and accuracy of data migration from RGMS to Sapphire (GMA and OmniGrants) will be verified using Technical and Business Verification', which will involve data matching.

Amendment of Personal Information by RAOs
As noted previously, an important feature of the current research granting and administration process is the apparent freedom given too many RAOs to populate and subsequently amend at any time the personal information held by NHMRC about researchers. It appears this can be done without direct reference back to the individual researcher on each occasion. Conceptually at least, this does represent a privacy risk in that the personal information held by NHMRC about an individual researcher may be amended without the individual's knowledge, with the potential that it becomes inaccurate.

In our opinion, a practical step that NHMRC could take in order to be reasonably satisfied that the information they hold about an individual (researcher) is accurate and up to date would be to contact all individuals on the Sapphire database by email on an annual basis, recommending they review their cv as held by NHMRC to ensure that it is accurate and up to date. This would dovetail neatly with a similar recommendation that we made above in respect of generally ensuring the accuracy of cvs/profiles.

Another step that NHMRC could take is to include, in a prominent place on Sapphire, a notice to individuals urging them to ensure that the personal information that NHMRC holds about them is accurate and up to date.

APP11 – Security of Personal Information

An agency must take reasonable steps to protect the personal information it holds from misuse, interference, loss, unauthorised access, unauthorised modification and unauthorised disclosure.

Analysis

The NHMRC Privacy Policy notes that, under the PGPA Act, NHMRC is required to implement the Australian Government Protective Security Policy Framework (PSPF). The PSPF is recognised as providing the appropriate controls for the Australian Government to protect its people, information and assets. All personal information held by NHMRC is stored in accordance with the PSPF and managed in accordance with the *Archives Act* 1983. Further, the policy also states that NHMRC complies with the Australian Signals Directorate Information Security Manual, 'and with relevant Government security standards when storing any information.'

The Privacy Policy also provides information and contact details for the NHMRC's Agency Security Advisor if an individual desires further information on the way NHMRC manages security risks in relation to personal information that it holds.

With respect to the security of the information held in Sapphire, the following information was provided:

Sapphire is being hosted on the Amazon Web Services (AWS) as a Software as a Service (SaaS)

OmniGrants (IT)

- The OmniGrants AWS tenancy uses the following ASD Certified Cloud Services: EBS, EC2, IAM, S3 and VPC.
- The OmniGrants AWS tenancy uses the following non-ASD Certified Cloud Services: Config, CloudFormation, CloudFront, CloudWatch, CloudTrail, Identity and Access Management (IAM), Route 53, SNS, SQS, SES.
- AWS APIs use the TLS encryption protocol to provide data transmission security.

GMA (IT)

- The GMA AWS tenancy uses the following ASD Certified Cloud Services: EBS, EC2, IAM, S3 and VPC.
- The GMA AWS tenancy uses the following non-ASD Certified Cloud Services: SNS, SQS.
- AWS APIs use the TLS encryption protocol to provide data transmission security.

Integration of the two systems is managed via a REST API. Messages sent by both providers are secured using a HMACSHA256 authentication header to ensure protection of messaged data and security of the system.

More generally, in relation to maintenance, Sapphire is a configurable system. Changes to Forms and Workflows will be provided to NHMRC to manage. Data Control and change governance is being put in place.

The key security risk to personal information held on Sapphire would appear to be:

- NHMRC staff obtaining or providing unauthorised access – deliberately or through ignorance;

- Third Party contractors securing or providing unauthorised access.

As noted above, Sapphire will sit within NHMRC's existing security framework, which is maintained in accordance with the requirements of the Australian Government Information Security Manual (ISM) and the Protective Security Policy Framework (PSPF).

The security procedures that are in place for each of the above risks are set out below:

NHMRC Staff

Most NHMRC staff who have access to RGMS and Sapphire in the future will only be provided with 'access to view' information on RGMS/Sapphire. Only a limited number will have 'edit' access.

There are different staff access levels, depending upon the role that the staff member may perform. They are Administrative, pre award and post award. Access to RGMS/Sapphire is provided to staff only after they have completed an online application. This identifies the level of access they require by requesting access similar to a named officer's level of access .

With respect to potential unauthorised access/manipulation by a staff member – the user interface records who has had access to any particular cv/record, and this assists in identifying any suspect access or unauthorised manipulation of personal information.

Training material is currently available on the NHMRC website for staff using RGMS, and an online training program is being developed for users of Sapphire.

We recommend that the NHMRC's training and delegations/authorisations regimes for staff and third party contractors using or having access to RGMS and, in the near future, Sapphire, should be more formally recorded. Currently, it appears to be somewhat informal.

The Sapphire system training provided to staff (and contractors) should be institutionalised within the agency's corporate management system.

We also recommend that a register of training provided to relevant staff (and also contractors) should be set up, along with a register of the varying levels of access approved to individual staff and contractors.

These features would assist in ensuring that all persons having access to Sapphire at varying levels are only permitted access when they have been properly trained and that NHMRC can properly track who has access to Sapphire from time to time.

More generally, these steps would improve the agency's accountability systems in this area.

Third Party Contractors

Contractors will have the ability to receive the same categories of access as NHMRC staff, depending upon the nature of the work they need to perform; *viz* Administrative, pre award and post award.

On the subject of security, the agreements with Semantics provide that the PSPF applies unless specified otherwise (cl 26 of GMA, and Sched 6 - Work Order 2017-18P62 c1-0). Separately, the agreements with F1 Solutions provide that the firm must develop a Data Protection Plan which covers personal information and which is consistent with the requirements of the Privacy Act as well as the PSPF and the Information Security Manual (cl 38.5 Contract Agreement v2.0).

These levels of security are satisfactory in the circumstances.

We note that the OAIC has in recent times been making public exhortations to agencies that, in using third party contractors for maintenance and upgrade work on their IT systems, they should ensure that the contractors are only provided with the level of access they need to undertake the work that is required, and not to provide them with unrestricted access to personal information held on the system. It is recommended that care should be taken to ensure that any arrangements for maintenance and upgrade work undertaken by third party contractors on Sapphire do not provide them with unrestricted access to the personal information contained in Sapphire unless it is considered absolutely necessary by NHMRC.

APP12 – Access to Personal Information

An agency must give an individual access to their personal information on request in accordance with the requirements of APP 12, unless an exception applies.

Analysis

A person can request access to any personal information in their record held by NHMRC.

The Privacy Policy confirms that an individual has a right of access to personal information that NHMRC may hold about them (subject to whether there is 'a(ny) law that allows or requires NHMRC to refuse access'). The Policy sets out the procedure that should be followed by an individual to secure such access. Essentially, it involves contacting the NHMRC's privacy officer by either email or postal address, the details of which are provided in the policy document.

With particular respect to personal information held by NHMRC on RGMS/Sapphire though, any researcher has direct access to their cv/profile anyway and so a researcher would not have to rely upon the APP 12 procedure to access their personal information held on the grants management system(s).

In any event, we have found nothing in the proposed implementation of Sapphire which would appear to narrow or restrict the existing access arrangements that are in place, and which we believe are satisfactory.

APP13 – Correction of Personal Information

An agency must take reasonable steps to correct a record of personal information if it is satisfied that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading ('unreliable').

Analysis

The Privacy Policy states that If a person requests that any part of their record be amended, then the NHMRC applies the general processes described on page 15 of its Privacy Policy to considering and, if approved,

amending the information. There is no prescribed form for this process, although an individual will be required to verify their identity before the request will be accepted. This is a statement of general process applicable to all and any personal information that NHMRC may hold though, and researcher cvs are in a different position.

With respect to personal information held on RGMS/Sapphire in relation to any researcher, we note that in practice, researchers have direct access through RGMS/Sapphire to their own personal information (cvs) anyway (see APP12 above) and can themselves (or through an approved RAO) correct their personal information without having to rely upon the APP 13 process.

We did note that APP 13.3 imposes a 30 day timetable on the processing of such requests. This is not stated in the Policy, whereas we note it is often set out in other agencies' privacy policies. We recommend that, when a review is held of the Policy in the future, consideration should be given to setting out more fulsomely the requirements of APP 13.3.

Otherwise, the existing processes comply with the requirements of APP 13, and nothing we have seen in the proposed implementation of Sapphire would appear to require a change to that existing framework.

END