PRIVACY IMPACT ASSESSMENT

FOR
MICROSOFT 365 AND AZURE IMPLEMENTATION

Contents

1. Executive Summary

1.1 Introduction

The National Blood Authority (NBA) has decided to upgrade its information and communications technology (ICT) infrastructure to cloud-based solutions using Microsoft 365, Microsoft Azure and Exclaimer:

- Cloud-based Microsoft 365 and Microsoft Azure services will deliver the following capabilities or services: email, calendar, directory, instant messaging, collaboration space, planning, Microsoft Teams, Microsoft Productivity suite (Word, Excel, PowerPoint, Access, Visio, and OneNote).
- A cloud-based version of Exclaimer software will manage and automatically add signature blocks to emails sent by NBA staff.

We recognise that cloud-based solutions raise potential privacy issues.

This Privacy Impact Assessment (PIA) explains the risk-based approach we undertook to analysing the key potential privacy risks of migrating some of our ICT infrastructure to the cloud, which includes assessing the project against the Australian Privacy Principles (APPs) in the *Privacy Act 1988*.

This PIA also sets out recommendations for managing, minimising or eliminating the key potential privacy risks identified in our analysis.

1.2 Findings and recommendations

Regarding openness and transparency, our analysis against the APPs found that amending our privacy policy and collection notices, to clearly state that personal information may be stored in a cloud, will ensure the project's compliance with the APPs 1, 3 and 5.

Regarding use of personal information, our analysis found that the project complies with APP 6. The project's privacy outcomes against APP 6 can be enhanced if we periodically seek assurances from Microsoft that it is not using NBA-owned personal information for any purpose other than providing us with infrastructure and cloud services. This would substantiate the contractual provisions around use of our information.

Regarding potential cross-border disclosure, the analysis found that the project complies with APP 8. The project's privacy outcomes against APP 8 can be enhanced by working with Microsoft to ensure any lawful request by an overseas authority seeking access to NBA information complies with the APPs and the Privacy Act.

Protecting and securing NBA-owned personal information is the biggest privacy risk of our project. The analysis found that strong privacy and security protections exist through a range of controls, which include contractual and security controls. In combination, these controls will adequately protect NBA-owned personal information from misuse, interference or loss, as well as unauthorised access, modification, or disclosure. These controls will ensure the project complies with APP 11 and achieve acceptable privacy outcomes.

A summary of recommendations based on our analysis is at Table 1. This includes a compliance check against key APPs based on NBA practices at April 2022 prior to implementing any recommendations.

Table 1: Summary of recommendations

APP	Commentary	Compliance check	Recommendation
APP 1 – open and transparent management of personal information	Current NBA privacy policy and some NBA privacy statements state that personal information will not be stored in a cloud	Not fully compliant, action required	1. Amend NBA privacy policy and privacy statements to indicate that personal information may be stored in a cloud 2. Publish and share this PIA.
APP 5 – notification of the collection of personal information	NBA collection notices indicate that personal information will not be stored in a cloud	Not fully compliant, action required	3. Amend NBA privacy collection notices to link to, or align with, the NBA's amended privacy policy
APP 6 – use or disclosure of personal information	There is a theoretical risk that Microsoft and its sub-processors could use NBA data for purposes outside the contractual framework	Compliant, action recommended to improve privacy outcomes	4. Seek assurances from Microsoft to substantiate the contractual arrangement that personal information will only be used for providing ICT services to the NBA.
APP 8 – cross border disclosure of personal information	Microsoft or its sub-processors may be required to disclose NBA data stored in Australian to an overseas authority under a relevant law	Compliant, action recommended to improve privacy outcomes	5. Ensure that Microsoft notifies the NBA of such an event and complies with the Privacy Act and APPs
APP 11 – security of personal information	Microsoft or its sub-processors could misuse, or make NBA data available for improper use.	Non-compliant, action recommended to ensure compliance with APP 11. Improper use of NBA information could undermine the NBA's ability to safeguard its information and put the NBA in breach of APP 11.	6. Implement multiple security controls to protect against improper use. 7. Monitor for departures from the Digital Transformation Agency blueprint or approved configurations. 8. Educate NBA staff on proper use of NBA information. 9. Seek assurances from Microsoft that it is safeguarding NBA information.

See the Table 2 in Appendix B for more details.

1.3 Conclusion

Moving our ICT infrastructure to the cloud is consistent with current government policy. We are committed to ensuring that our move to the cloud achieves an appropriate balance between ICT efficiency and privacy.

Our analysis identified that data security in relation to Microsoft 365 and Azure poses the greatest potential privacy risk for this project. A failure to ensure the security of our data (including personal information) could cause harm to impacted individuals and harm our reputation.

Our contractual arrangements with Microsoft include requirements for Microsoft to comply with Commonwealth protective frameworks, the Privacy Act and the APPs. They are robust to ensure the NBA maintains effective control over its data including NBA-owned personal information.

We can also implement internal security controls to restrict internal access of personal information and to protect against unauthorised access, modification or disclosure. We can monitor the cloud-based services for any departures from our approved configuration. We can periodically seek assurances from Microsoft that it is safeguarding our information consistent with the contractual framework.

Overall, we have concluded that by implementing a range of controls available to us, we can adequately protect the personal information we hold from misuse, interference or loss, as well as unauthorised access, modification or disclosure. We consider the controls sufficient to ensure the project's compliance with APP 11 and to achieve acceptable privacy outcomes for our project.

Other potential privacy risks highlighted in this PIA can be adequately mitigated:

- We can update our privacy policy and collection notices to clearly indicate that personal information may be stored in a cloud, to ensure compliance with APPs 1 and 5.
- We can implement the additional controls recommended in the analysis to improve the project's privacy outcomes against APPs 6 and 8.

We have concluded that the potential privacy risks of upgrading to a cloud-based solution using Microsoft 365, Azure and Exclaimer can be adequately managed by implementing all the recommendations outlined in this PIA.

We are of the view that storing and processing our data within Microsoft's cloud services within Australia is safe, effective and does not put NBA-owned personal information at undue privacy risk.

The NBA will publish this PIA on its PIA Register at https://www.blood.gov.au/privacy. By the time of publication, the NBA is expected to have implemented many of the recommendations set out in this PIA.

This PIA reflects circumstances in April 2022 when the analysis was conducted.

2. What is a privacy impact assessment?

A PIA assesses the privacy impacts of new or amended projects or processes. A PIA also identifies way in which potential privacy risks can be mitigated and positive impacts enhanced.

The Privacy Act requires APP entities to protect 'personal' and 'sensitive' information according to the thirteen APPs which cover the collection, use, storage and disclosure of personal information and an individual's access to, and correction of, that information.

The Privacy Act (section 6) defines 'personal information' as:

> '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.'

'Sensitive information' is a subset of personal information. The Privacy Act (section 6) defines 'sensitive information' as:

> '(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
> (ix) 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.'

A PIA must be prepared when considering or undertaking any of the following activities:

- new or existing projects
- changes to processes or procedures
- policy proposals
- initiatives, programs or activities
- new or amended technology, systems, or databases
- new procedures involving overseas entities or disclosures of personal information to overseas recipients are being considered.

3. PIA process

This PIA follows the 10-step process recommended by the Office of the Australian Information Commissioner for analysing privacy impacts.

All NBA business areas are affected by this project. Consultations with all NBA business areas through the NBA's senior management group occurred in April 2022. Feedback obtained from these consultations assisted with clarifying the types of personal information collected and held by the NBA and how personal information is collected. Feedback also tested whether the proposed mitigation strategies are appropriate. The consultations did not raise any significant concerns.

The following factors are also relevant factors to the NBA's project and this PIA:

- The Australian Government's 'cloud first' policy when adopting new or updating existing ICT services
- The Australian Digital Transformation Agency's Protected Utility Blueprint at: https://desktop.gov.au/
- Australian Cyber Security Centre: Cloud Computing Security Considerations at: https://www.cyber.gov.au/acsc/government/cloud-security-guidance
- Attorney-General's Department's Protective Security Policy Framework at: https://www.protectivesecurity.gov.au/policies
- Office of the Australian Information Commissioner's Guide to Securing Personal Information at: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information
- Office of the Australian Information Commissioner's Guide to Undertaking Privacy Impact Assessments at: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments
- Cloud Computing and Information Management information published by National Archives of Australia at: Cloud computing and information management | naa.gov.au

4. Project description

4.1 What is the project?

Our current infrastructure utilises Microsoft Office productivity tools with our data and applications hosted on-premises. These systems are outdated and are coming under increasing strain.

We have decided to upgrade to cloud-based Microsoft 365 and Microsoft Azure services to deliver the following capabilities or services: email, calendar, directory, instant messaging, collaboration space, planning, Microsoft Teams, Microsoft Productivity suite (Word, Excel, PowerPoint, Access, Visio, and OneNote). This will improve the NBA's ability to deliver core services efficiently and effectively.

The upgrade involves migrating our email data and the 'documents' folder of our staff to Microsoft's cloud environment. Data to be migrated includes personal or sensitive information – for example, patient information received or sent via email, human resources information about NBA staff.

The project also involves upgrading to a cloud-based version of Exclaimer software, a solution that works using the Microsoft Azure cloud platform. We currently use Exclaimer software for the management and automatic addition of signature blocks to emails sent by NBA staff.

The scope of the project is to:

- deploy laptops to all NBA staff that will utilise Microsoft 365 applications
- configure and provide access to cloud-based Microsoft productivity tools including email services
- migrate existing email from on-premises email servers to the NBA tenancy in the Microsoft Azure cloud service
- migrate documents in the 'documents' folder of NBA staff from on-premises servers to the NBA tenancy in the Microsoft Azure cloud service
- implement the cloud-based Exclaimer service for management and automatic addition of signature blocks to emails.

Two key environmental factors impact this project.

- The requirement to protect privacy in compliance with the Privacy Act including the 13 APPs.
- The direction and guidance by the Commonwealth of Australia to agencies to adopt a 'cloud first' approach when replacing ICT infrastructure, applications or services because they are understood to be more cost effective and agile than on-premises internal ICT infrastructure.

4.2 What are the aims or objectives of the project?

The principal objectives of the project are to:

- provide our staff with an improved experience when using Office productivity and collaboration tools that allow them to work more effectively internally and with external parties
- enable staff to work from anywhere at any time using an NBA issued device
- improve the security of our ICT infrastructure
- reduce ICT complexity and operating costs.

4.3 Who is responsible for the project?

The NBA Deputy Chief Executive, Fresh Blood Products and Business Systems.

4.4 What personal information is impacted by this project?

The personal information described in Appendix A collected or held within the Microsoft 365 and Azure services and applications.

Personal information held in our digital document management system will continue to be stored on-premises, unchanged by this project.

4.5 Where will NBA data be stored under the project?

Storage of NBA data is restricted to the geographic region of Australia.

Our NBA data will be retained and managed within Microsoft data centres in Australia. These data centres are located in Canberra, Sydney and Melbourne (Source: https://azure.microsoft.com/en-us/global-infrastructure/geographies/#geographies, dated 09/06/2022).

At the time of finalising this PIA it is understood the following Microsoft 365 services are hosted in Australia:

- Exchange Online
- OneDrive
- SharePoint Online
- Microsoft Teams
- Office Online and Mobile
- Planner
- OneNote Services
- Stream
- Viva Connections
- Viva Insights - Personal
- Whiteboard.

(Source : https://docs.microsoft.com/en-us/microsoft-365/enterprise/o365-data-locations?view=o365-worldwide, dated 17/03/2022)

The Exclaimer cloud service used by the NBA is hosted in the Microsoft Azure cloud service in Australia. The Terms of Use of the Exclaimer service restrict the service to operating within the cloud region nominated by the NBA, which is the Australia region of Microsoft Azure.

5. Privacy Impact Analysis

Most of our privacy practices will remain the same under the upgrade to Microsoft 365, Azure and Exclaimer. The main change is to how we store and process our data.

The project will involve Microsoft storing and processing our data (including personal information) in new ways, which involves us relinquishing some control over our data. This raises privacy risks for consideration in this PIA.

This section of the PIA is our analysis of the project against APPs relevant to this project, including recommended strategies to improve the project's privacy outcomes. The analysis provides the basis on which we can determine whether the project has acceptable or unacceptable privacy impacts.

A summary of the key privacy risks and recommended risk mitigation strategies based on our analysis is in Table 2 of Appendix B.

5.1 Open and transparent management of personal information

APP 1 – open and transparent management of personal information.

The NBA must have ongoing practices and policies in place to ensure that it manages personal information in an open and transparent way. The NBA must:

- take reasonable steps to implement systems to comply with the APPs
- have a clearly expressed and up-to-date privacy policy about how it manages personal information
- make its privacy policy freely available.

Our privacy policy states that the NBA will not store personal information in a cloud. The project will involve some NBA-owned personal information being stored in a cloud. Some information will continue to be store on premises.

To ensure the project's compliance with APP 1 and acceptable privacy outcomes, we need to amend our privacy policy to clearly state that personal information may be stored in a cloud. This will ensure transparency about how we store personal information – that is, it may be stored in a cloud (if impacted by this project) or remain on-premises.

We can improve the project's privacy outcomes by publishing this PIA on the NBA's PIA register. This will openly demonstrate that privacy issues have been in considered in this project.

We can enhance the project's privacy outcomes by sharing this PIA with our staff as part of their ongoing privacy awareness training. Our employment policies include a requirement for all our staff to undertake mandatory privacy awareness training annually.

5.2 Collection of personal information

APP 3 – collection of personal information

Any personal information the NBA collects (including sensitive information) must be reasonably necessary for, or directly related to, one or more of the NBA's functions or activities.

The NBA cannot collect sensitive information about a person unless they consent and the information is reasonably necessary for, or directly related to, one or more of our functions or activities, or one of the exceptions in APP 3.4 applies.

Personal information can only be collected by lawful and fair means.

Personal information about a person can only be collected from that person, and not from anyone else, unless one of the exceptions in APP 3.6 applies.

APP 5 – notification of the collection of personal information

When the NBA collects personal information, it must notify the individual or otherwise ensure they are aware of, the matters listed in APP 5.2. These matters include:

- the NBA's identity and contact details
- the fact and circumstances of the collection (if personal information has been collected from someone other than the person and the person may not be aware of this)
- whether collection is required or authorised by law
- the purposes for which the information is collected
- the main consequences, if any, for the individual if the personal information is not collected
- who the NBA usually discloses the personal information to
- information about the NBA's Privacy Policy – how individuals can access and correct their personal information and how they can complain about a breach of their privacy
- whether the NBA is likely to disclose personal information to people or organisations overseas and if so, the countries in which those people or organisations are located (if practicable).

We will continue to collect personal information only for purposes directly related to our statutory functions set out in the *National Blood Authority Act 2003* (section 8) and as described in the NBA's privacy policy. This is unchanged by the project.

Our functions include liaising with data stakeholders in the blood sector and gathering information (known as 'blood sector data') to:

- monitor the demand for blood and blood products
- undertake annual supply and production planning and budgeting
- undertake or facilitate national information management, benchmarking and cost and performance evaluation for the national blood supply.

We collect personal information through:

- the MyABDR app (used by patients to record home treatment and bleeds and manage treatment stock)
- the Blood Portal
- emails or email attachments
- hard copy documents that are subsequently scanned
- in person contacts and telephone discussions
- the NBA website using a 'cookie'.

We collect personal information directly from individuals with their consent – for example, the BloodPortal, MyABDR.

We also receive personal information provided to us by third parties such as health organisations and professionals (which forms part of our blood sector data holdings). The third party supplying the information will have obtained the individual's informed consent prior to disclosing their personal information to us. The third party will also have informed the individual where they can view the NBA's privacy policy.

The project will not directly impact MyABDR or the BloodPortal as personal information in those systems will continue to be stored on our premises. However, personal information can be extracted from those systems and used in a way that is impacted by the project – for example, if personal information is extracted and shared via email, or stored on a file directory within our corporate systems. We consider that the extraction of personal information from MyABDR and BloodPortal raises potential privacy risks and warrants consideration in this PIA.

NBA privacy policy

Our privacy policy states that we do not store personal information in a cloud. As indicated in the analysis relating to APP 1, we need to amend our privacy policy. Once amended and published, the policy will serve as an up-front statement about how we manage personal information including the possibility of storage in a cloud.

In our privacy notices relating to specific NBA functions, we typically include a link to our privacy policy. The amended privacy policy will contribute to the project's compliance with APP 5 as described below.

The BloodPortal, BloodNet and BloodSTAR

The BloodPortal is a secure, central user management and authentication system which provides access to our ICT blood sector systems, BloodSTAR and BloodNET. Access to the BloodPortal is subject to the user accepting the user terms and conditions, which serves as a notice for the purposes of APP 5. The terms and conditions are silent on cloud storage but include a link to our privacy policy for information on how the NBA manages personal information.

BloodSTAR is online system used across Australia to manage access to government funded immunoglobulin products. The BloodSTAR privacy statement and notice, available at https://www.blood.gov.au/bloodstar-privacy-controls, outlines how personal information is managed within the system without referring to how information is stored. The statement defers to our privacy policy for more details on how we manage personal information generally.

BloodNET is an online blood ordering and inventory management system that allows staff in health facilities across Australia to order blood and products from Australian Red Cross Lifeblood. BloodNET's terms user terms and conditions serve as a notice for the purposes of APP 5 and state that personal information is managed in accordance with our privacy policy.

Amending our privacy policy to state that personal information may be stored in a cloud will ensure that the BloodPortal, BloodSTAR and BloodNET comply with APP 5.

MyABDR app and ABDR

MyABDR is an internet based online system for individuals to:

- record treatments and bleeds
- manage treatment product stock
- share information with their haemophilia centre through the Australian Bleeding Disorders Registry (ABDR)
- update contact and personal details.

A user registers for the MyABDR app or ABDR after providing their informed consent. The ABDR and MyABDR privacy policy and consent form are at https://www.blood.gov.au/privacy-info-abdr-myabdr. Although neither document states where we store personal information, they both include a link to our privacy policy.

Updating our privacy policy to clearly state that personal information may be stored in a cloud will ensure that the privacy policy and consent forms for ABDR and MyABDR comply with APP 5.

Blood sector data

We collect, analyse, report, publish and hold blood sector data as part of our statutory functions. We manage blood sector data according to governance principles and arrangements under the NBA Data and Information Governance Framework.

Blood sector data includes sensitive (health) information about individuals provided directly to us through MyABDR or Blood Portal, or which has been provided to us through trusted third parties under the framework.

Only some personal information provided to us under the framework is impacted by the project:

- Personal information shared by email is impacted by this project - for example, data requests having minimal or low privacy impact may be dealt with by email.
- Data without aggregation and other high privacy risk data is usually shared through the sharing platform Objective Connect and is not impacted by this project.

Appendix 11 of the framework outlines the security arrangements for storing of blood sector data, and currently indicates we physically host all data infrastructure with no cloud-based storage. To ensure compliance with APP 5 we need to amend Appendix 11 to clearly indicate that personal information may be stored in a cloud.

Conclusion

The purposes for which we collect personal information (including sensitive information) to fulfil our statutory functions will continue to comply with APP 3 and achieve acceptable privacy outcomes.

Amending our privacy policy to clearly state that personal information may be stored in a cloud will ensure that users of the BloodPortal, BloodNET, BloodSTAR, ABDR and the MyABDR app are properly informed about why we collect their personal information and how it may be stored.

Amending the NBA Data and Information Governance Framework as described will ensure that impacted individuals are properly informed about why we collect their personal information and that the NBA may store their personal in a cloud.

These amendments will ensure compliance with APP 5 and achieve acceptable privacy outcomes for our project.

5.3 Use of personal information

APP 6 – use or disclosure of personal information

The NBA can only use or disclose personal information for the purpose for which it was collected (the 'primary purpose'). Personal information cannot be used or disclosed for another purpose ('secondary purpose') unless the person consents or one of the exceptions in APP 6.2 applies.

We use personal information to undertake our functions and activities. We will continue to use personal information as described in our privacy policy, unchanged by the upgrade to a cloud platform.

If personal information is collected for a specific purpose, we will only use it for that purpose, unless an exception under the Privacy Act applies. We will only use personal information for a secondary purpose where consent has been provided or an individual would reasonably expect us to use the information for the secondary purpose.

Microsoft 365 and Azure

The project will involve Microsoft and its sub-processors having access to NBA-owned personal information to provide the following capabilities or services to the NBA: email, calendar, directory, instant messaging, collaboration space, planning, Microsoft Teams, Microsoft Productivity suite (Word, Excel, PowerPoint, Access, Visio, and OneNote).

These capabilities facilitate official communications and allow staff and external parties to share information electronically. Effective communication is essential to delivering our functions under the National Blood Authority Act.

Our contractual framework with Microsoft provides for NBA-owned personal information to be used or accessed only for the purposes of delivering services in accordance with the contractual framework and for no other purposes. We consider the contractual provisions adequate to comply with APP 6.

By allowing Microsoft and its sub-processors to process and store our personal information, we could be exposing the personal information we hold to an increased risk of misuse. A failure to ensure our data Is not misused could harm affected individuals, our data stakeholders and could adversely impact our reputation.

We can mitigate the risk of misuse of NBA-owned personal information by periodically seeking assurances from Microsoft to substantiate the contractual arrangements that NBA-owned information will used only for the purpose of delivering the agreed ICT services to the NBA. Seeking these assurances will strengthen compliance with APP 6 and improve the project's privacy outcomes.

Exclaimer

Our contractual framework with Exclaimer involves a licensing agreement that contains a range of controls applied by Exclaimer to ensure the security of NBA-owned personal information. This includes access controls to prevent NBA-owned personal information from being used for a purpose other than the application of electronic signatures to NBA emails.

Also, a key control against unauthorised use of our information is that the contents of NBA emails will be encrypted and therefore inaccessible when passed to Exclaimer's cloud-based service for the addition of a signature block.

We consider the controls in the licensing agreement and the encryption control sufficient to ensure the project's compliance with APP 6 and to achieve acceptable privacy outcomes.

5.4 Cross-border disclosure of personal information

APP 8 – cross-border disclosure of personal information

If the NBA discloses personal information to a person or organisation overseas, the NBA is accountable for any privacy breaches committed by the overseas person or organisation (see section 16C of the Privacy Act).

Therefore, before the NBA discloses personal information to a person or organisation overseas, the NBA must take reasonable steps to ensure they do not breach the APPs in relation to the information, unless one of the exceptions in APP 8.2 applies.

Microsoft is an American based provider. When data is shared with Microsoft for storing or processing on the NBA's behalf, we will relinquish some control over our personal information. We will, however, maintain effective control over our data through the contractual framework. This will include:

- a requirement that Microsoft comply with the Privacy Act including the APPs
- a requirement that Microsoft comply with all Australian Government policies. Currently the policies relevant for securing personal information are the Commonwealth Protective Security Policy Framework at http://www.protectivesecurity.gov.au and the Information Security Manual at http://www.asd.gov.au/infosec/ism/index.htm
- a requirement that Microsoft comply with any notified NBA policies.

We will be implementing security controls to ensure that our data remains within Australia – see **5.5 Data Security.**

The combination of contractual provisions and security controls provides us with meaningful control over our data while it is processed and stored by Microsoft on our behalf.

Our level of control over our data means that will not be 'disclosing' personal information to Microsoft for the purposes of APP 8. Retaining control is important so that we can properly mitigate privacy risks and ensure that we remain compliant with our obligations under the Privacy Act and the APPs.

Our use of an overseas provider slightly increases the likelihood of our data being subject to an overseas law enforcement request even though our data is stored in Australia. The likelihood of this occurring is extremely low. However, it could undermine our ability to effectively control our data, and harm individuals impacted by the request (if it involves their personal information).

We can mitigate risk by seeking assurances from Microsoft that we will be notified of a request to disclose NBA-owned information, and that any lawful request will be dealt with according to the contractual framework including compliance with the APPs. Seeking these assurances will strengthen compliance with APP 8 and improve the project's privacy outcomes.

In relation to Exclaimer, there is no disclosure of personal information to warrant action relating to APP 8. NBA emails are encrypted before they are passed to Exclaimer for the addition of a signature block. Exclaimer will not access NBA-owned personal information.

5.5 Data security

APP 11 – security of personal information

The NBA must take reasonable steps to protect personal information it holds from misuse, interference or loss, as well as unauthorised access, modification, or disclosure.

When an APP entity no longer needs personal information, it must take reasonable steps to destroy the information or ensure that the information is de-identified, unless an exception applies.

Data security is the biggest privacy risk for this project. A failure to ensure the security of our data (including personal information) could cause harm to our impacted individuals and harm our reputation.

We have assessed the security of Microsoft 365, Azure and Exclaimer against our specific risks and requirements, including the requirement to comply with the Commonwealth Protective Security Policy Framework (PSPF) and the Information Security Manual (ISM).

The PSPF consists of 16 policies on security governance, information security, personnel security and physical security.

The ISM consists of 24 principles that provide strategic guidance on protecting systems and data from cyber threats. These principles can be grouped as follows.

- Govern: identifying and managing security risks.
- Protect: implementing security controls to reduce security risks.
- Detect: detecting and understanding cyber security events to identify cyber security incidents.
- Respond: responding to and recovering from cyber security incidents.

The contractual framework for Microsoft 365, Azure and Exclaimer:

- requires the service providers to comply with all Australian policies and laws applicable to the services (which includes the PSPF, ISM and the Privacy Act)
- provides that the suppliers will not acquire any rights in our data
- requires the service provider to only use or disclose our data for the following purposes:
    - to provide us with the Microsoft 365, Microsoft Azure, and Exclaimer services
    - where required by law, for law enforcement purposes.

We consider the range of security protections under the contractual framework to be a sound basis for protecting NBA-owned personal information.

We also have existing controls to mitigate against the risk of misuse, interference or loss as well as unauthorised access, modification, or disclosure. These are discussed below.

Restricting access to certain personnel

Information stored within Microsoft 365 services is only generally available to our staff and only from NBA-secured devices.

Our staff (including contract staff) are granted access to NBA-owned personal information only if there is a business need and subject to approval by a senior NBA official. Access automatically ceases when their NBA employment or engagement ends.

Microsoft personnel will not have standing access to our information. In the rare event that Microsoft personnel require access information within our infrastructure (for example, for service fault diagnosis and restoration), they will require us to approve and enable their access to our systems.

Access to information within Microsoft 365 services is logged and can be audited. Microsoft 365 and Azure offer the ability to monitor suspicious activity with reporting, auditing, and alerts, and to mitigate potential security issues.

The personal information provided to Exclaimer is only that required to allow Exclaimer to provide services to the NBA – that is, the information of our staff to be included in signature blocks such as name, phone number, position and NBA postal address.

Information security controls

In configuring the cloud-based services provided under this project, we will follow the Digital Transformation Agency's Protected Utility Blueprint (https://desktop.gov.au/). The blueprint is a pattern that government agencies can use to implement a secure, modern desktop based on Microsoft 365, which complies with the Australian Government Information Security Manual (https://www.cyber.gov.au/acsc/view-all-content/ism).

Our configuration will:

- restrict NBA held data to being stored within Australia
- require access to our data by Microsoft to be approved by us.

If necessary, we will depart from the blueprint to meet our business purposes. Any departures will have no privacy impacts relating to NBA-owned personal information.

The NBA will also utilise Perimeta for Azure and Perimeta for 365 software to monitor the configuration of the cloud-based services. This enables us to identify any instance where the configuration does not comply with the blueprint or our approved configuration, and to take appropriate remedial action.

We consider that Microsoft 365, Microsoft Azure and Exclaimer, configured in compliance with the blueprint, provides a secure environment that meets our needs and adequately protects the privacy of our data.

Controls against unauthorised access, modification or disclosure

We use a range of measures to protect NBA-owned personal information from unauthorised access, modification or disclosure, including:

- security vetting for all staff who will have access to our systems and/or information
- security arrangements to ensure access controls, audit logging and other treatments or controls are implemented to prevent unauthorised access to personal information
- auditing Microsoft's compliance with security arrangements
- controls to ensure notification and reporting of any breaches.

We require our staff and service providers (who need access to our ICT infrastructure) to follow the NBA's ICT conditions of use policy to ensure ethical, appropriate and secure use of our infrastructure. Inappropriate use can result in disciplinary action including termination of employment or engagement.

If a data breach is reported or detected, it will be handled according to our data breach response plan.

We consider that there is a minimal risk of harm from unauthorised access, modification or disclosure of personal information by Microsoft or Exclaimer.

Retention of information

The personal information we collect forms part of a Commonwealth record. The APP 11.2 requirement to destroy or de-identify personal information does not apply to information contained in a Commonwealth record.

Retention, destruction and alteration of Commonwealth records is governed by the *Archives Act 1983*.

Conclusion

There will be a range of controls in place to provide strong privacy and security protections for our data including NBA-owned personal information. The controls comprise of contractual provisions, the application of the Privacy Act and the APPs and internal security controls.

Overall, we are satisfied that implementing these controls will adequately protect the personal information we hold from misuse, interference or loss, as well as unauthorised access, modification or disclosure.

We consider the controls sufficient to ensure the project's compliance with APP 11 and to achieve acceptable privacy outcomes for our project.

To enhance the project's privacy outcomes against APP 11, we should periodically seek assurances from Microsoft that it is safeguarding our information consistent with the contractual framework.

Appendix A – Personal Information

The personal information affected by this project includes sensitive health information of individuals within and outside the NBA. An indicative list of personal information held by the NBA is:

(1) Title, given and last name
(2) Contact details – address, email, and phone number
(3) Health information about an individual.

The personal information of NBA staff affected by this project is information related to the individual's employment or contract. An indicative list of the types or records that the NBA hold which contain information is:

(1) identification documents
(2) records relating to attendance and overtime
(3) leave applications and approvals
(4) medical and dental records
(5) payroll and pay related records, including banking details
(6) superannuation information
(7) other financial information of employees including in relation to novated leases
(8) tax file number declaration forms
(9) declarations of pecuniary interests
(10) personal history files
(11) performance appraisals etc
(12) records relating to personal development and training
(13) trade, skill, and aptitude test records
(14) completed questionnaires and personnel survey forms
(15) records relating to removals
(16) travel documentation
(17) records relating to personal welfare matters
(18) contracts and conditions of employment
(19) diversity data
(20) emergency contact details
(21) next of kin details
(22) recruitment records including security clearances
(23) records of accidents and injuries
(24) compensation and/or rehabilitation case files
(25) records relating to counselling and discipline matters, including disciplinary, investigation and action files, legal action files, records of criminal convictions, and any other staff and establishment records as appropriate
(26) complaints and grievances
(27) recommendations for honours and awards.

Appendix B – Privacy risks and management

Key privacy risks of the project have been identified and assessed against the 13 APPs by applying the following risk matrix.

+

Likelihood	Consequence			
	Extreme	High	Medium	Low
Almost certain	Extreme – Business Committee Management	Extreme – Business Committee Management	High – Deputy Chief Executive Management	Medium – Director Management
Likely	Extreme – Business Committee Management	Extreme – Business Committee Management	High – Deputy Chief Executive Management	Medium – Director Management
Possible	High – Deputy Chief Executive Management	High – Deputy Chief Executive Management	Medium – Director Management	Low – Routine Staff Management
Unlikely	Medium – Director Management	Medium – Director Management	Low – Routine Staff Management	Low – Routine Staff Management

Table 2: Privacy impact analysis and compliance check as at April 2022

APP 1: open and transparent management of personal information						
Do we have a clearly expressed and up-to-date privacy policy?	Description of the identified risk	Compliance check	Initial Risk Rating	Recommended risk mitigation strategy	Final risk rating	Risk owner
Our Privacy Policy states that personal information will not be stored in a cloud and that personal information will only be stored within Australia. Some privacy statements within our ICT blood sector systems indicate that personal information will not be stored in a cloud.	Consent from individuals may not be valid if based on inaccurate information. This could result in complaints or harm our reputation.	Not fully compliant, action required. Failure to provide accurate information could put us in breach of APP 1.	Extreme Likelihood: Almost certain Consequence: High	Amend our privacy policy and relevant privacy statements to indicate that personal information will be stored in the cloud. Publish this PIA on our PIA register. Share with staff to improve privacy awareness.	Low Likelihood: Unlikely Consequence: Low	Privacy Officer

APP 2: anonymity and pseudonymity						
Will individuals have the option of not identifying themselves, or using a pseudonym, when dealing with us?	Description of the identified risk	Compliance check	Initial Risk Rating	Recommended risk mitigation strategy	Final risk rating	Risk owner
Generally, the purposes for which we collect personal or sensitive information requires the person to be identifiable. A pseudonym may be used for identification in the Australian Bleeding Disorders Registry.	The move to cloud-based Microsoft 365, Azure and Exclaimer does not impact on compliance with APP 2.	N/A	N/A	N/A	N/A	N/A

APP 3: collection of solicited personal information						
Is the personal information reasonably necessary for, or directly related to, our functions or Activities?	Description of the identified risk	Compliance check	Initial Risk Rating	Recommended risk mitigation strategy	Final risk rating	Risk owner
We only collect personal information when it is directly related to our statutory functions. Sensitive information is only collected with the individual's consent or where a legal exception applies.	The move to cloud-based Microsoft 365, Azure and Exclaimer does not impact on compliance with APP 3.	N/A	N/A	N/A	N/A	N/A

APP 4: dealing with unsolicited personal information						
Are there systems in place for dealing with unsolicited personal information?	Description of the identified risk	Compliance check	Initial Risk Rating	Recommended risk mitigation strategy	Final risk rating	Risk owner
Rarely received, it will be dealt with case-by-case having regard to the context in which the information was provided.	The move to cloud-based Microsoft 365, Azure and Exclaimer does not impact on compliance with APP 4.	N/A	N/A	N/A	N/A	N/A

APP 5: notification of the collection of personal information						
Does the NBA take reasonable steps to notify the individual of the matters listed in APP 5.2?	Description of the identified risk	Compliance check	Initial Risk Rating	Recommended risk mitigation strategy	Final risk rating	Risk owner
Our privacy collection notices usually contain a link to our privacy policy or state that personal information will not be stored in a cloud.	Consent from individuals may not be valid if based on inaccurate information. This could result in complaints or harm the NBA's reputation.	Not fully compliant, action required. Failure to provide accurate information in a privacy collection notice could put the NBA in breach of APP 5.	Extreme Likelihood: Almost certain Consequence: High	Amend the NBA's privacy collection notices to link to, or align with, the updated Privacy Policy.	Low Likelihood: Unlikely Consequence: Medium	Privacy Officer and responsible line managers

APP 6: use or disclosure of personal information						
How do we ensure that personal information is used only for the purpose for which it was collected?	Description of the identified risk	Compliance check	Initial Risk Rating	Recommended risk mitigation strategy	Final risk rating	Risk owner
Our privacy policy states how we will use personal information - that is, to fulfil our functions and activities or for a specified purpose. Contractual provisions require Microsoft and its sub-processors to use personal information only for the purposes of the agreement.	Microsoft or its sub-processors could use personal information for other purposes outside of its arrangement with us. This could result in complaints or harm our reputation.	Compliant, action recommended to improve privacy outcomes. Unauthorised use of personal information could breach APP 6.	Medium Likelihood: Possible Consequence: Medium	Seek assurances from Microsoft periodically to substantiate contractual provisions that personal information will only be used consistent with the contract.	Low Likelihood: Unlikely Consequence: Medium	Chief Information Officer

APP 7: direct marketing						
What systems do we have in place to manage its direct marketing obligations under the Privacy Act?	Description of the identified risk	Compliance check	Initial Risk Rating	Recommended risk mitigation strategy	Final risk rating	Risk owner
The NBA does not use or disclose personal information for direct marketing. The contract requires Microsoft to use personal information only for the purposes of the agreement (see APP 6).	The move to cloud-based Microsoft 365, Azure and Exclaimer does not impact on compliance with APP 7.	N/A	N/A	N/A	N/A	N/A

APP 8: cross border disclosure of personal information						
What reasonable steps can the NBA take to ensure that an overseas recipient of personal information does not breach the APPs?	Description of the identified risk	Compliance check	Initial Risk Rating	Recommended risk mitigation strategy	Final risk rating	Risk owner
Under the contractual arrangement with Microsoft, the NBA will retain effective control over its data. The contract requires Microsoft to comply with the APPs, Commonwealth policies and any notified NBA policies. Current Commonwealth policy requires that data be stored within Australia.	Despite the NBA's effective control over the data, Microsoft may be required to disclose the NBA data stored in Australia to an overseas authority under a relevant law.	Compliant, action recommended to improve privacy outcomes. Any lawful disclosure could be perceived as non-compliance with APP 8.	High Likelihood: Possible Consequence: Medium	Seek assurances from Microsoft that it will notify the NBA of such a request and manage a request according to the APPs and Privacy Act (per contractual obligations). Monitor for changes to policy requirement to store data within Australia and consider the NBA's response options.	Medium Likelihood: Unlikely Consequence: Medium High	Chief Information Officer

APP 9: adoption, use or disclosure of government identifiers						
Does the project extend the adoption, use or disclosure of government related identifiers??	Description of the identified risk	Compliance check	Initial Risk Rating	Recommended risk mitigation strategy	Final risk rating	Risk owner
The NBA assigns its own identifiers for internal purposes. It also discloses government identifiers of its staff to the Department of Health for payroll purposes. This will not change under the project. The objective of APP 9 is to restrict use of government related identifiers so that they do not become universal identifiers.	The move to Microsoft 365, Azure and Exclaimer will not impact on compliance with APP 9.	N/A	N/A	N/A	N/A	N/A

APP 10: quality of personal information						
Will reasonable steps be taken to ensure accuracy etc. of personal information?	Description of the identified risk	Compliance check	Initial Risk Rating	Recommended risk mitigation strategy	Final risk rating	Risk owner
The NBA must take reasonable steps to ensure that the personal information it collects is accurate, up-to-date, and complete before using or disclosing it.	The move to Microsoft 365, Azure and Exclaimer will not impact on compliance with APP 10.	N/A	N/A	N/A	N/A	N/A

APP 11: security of personal information						
Will reasonable steps be taken to protect personal information held by the NBA from misuse, interference, loss as well as unauthorised access, modification or disclosure?	Description of the identified risk	Compliance check	Initial Risk Rating	Recommended risk mitigation strategy	Final risk rating	Risk owner
The NBA considers that Microsoft and Exclaimer offer a range of security protections that meet the NBA's requirements to effectively protect against improper use of NBA data including personal information.	Microsoft or its sub-processors could misuse, or make NBA data available for improper use, contrary to it arrangement with the NBA.	Non-compliant, action recommended to ensure compliance with APP 11. Improper use of NBA information could undermine the NBA's ability to safeguard its information and put the NBA in breach of APP 11.	Medium Likelihood: Possible Consequence: Medium	Implement range of security controls, including: - procedures for NBA approving Microsoft access - configure rules to identify and prevent sending of certain information - restrict access to NBA controlled devices or apps - audit Microsoft's compliance with security arrangements - security vetting of staff. Perimeta software to monitor for departures from the DTA blueprint or approved configurations. Educate NBA staff on proper use of NBA information. Periodically seek assurances from Microsoft that it is safeguarding NBA information	Low Likelihood: Unlikely Consequence: Medium	Chief Information Officer

APP 12: access to personal information

APP 13: correction of personal information

Does the NBA provide for individuals to access and correct their personal information?	Description of the identified risk	Rationale and consequences for the NBA	Initial Risk Rating	Recommended risk mitigation strategy	Final risk rating	Risk owner
The NBA's Privacy Policy sets out how an individual can access and seek correction of their personal information. It includes information about how to complain about a breach of privacy.	The move to Microsoft 365, Azure and Exclaimer will not impact on compliance with APP 13.	N/A	N/A	N/A	N/A	N/A