VOKKE

Discover. Build. Disrupt.

Vokke Australia
Spaces in Rialto Towers,
525 Collins St,
Melbourne, Vic, 3000
Australia

Vokke Philippines
Level 7, Lepanto Building,
8747 Paseo de Roxas, Makati,
Metro Manila
Philippines

AADPA ADHD Tracker

PRIVACY IMPACT ASSESSMENT SUMMARY

Version 1.0

Published 30/09/2020

Executive Summary

This report outlines the process and outcomes of a Privacy Impact Assessment (PIA) undertaken for the AADPA 'ADHD Tracker' system, as developed by Vokke. The PIA was conducted collaboratively between Vokke and AADPA. This document has been constructed based on the OAIC's for undertaking a PIA. https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/#undertaking-a-pia

About this document

This PIA report has been created as a public-facing version of a Privacy Impact Assessment that was conducted by Vokke and AADPA. Project stakeholders may access a more detailed version of the PIA by contacting Vokke.

Accuracy

All attempts are made to ensure the information is accurate as of the time of publication, although please note that the authors place no guarantee on the timeliness or accuracy of the information. For up-to-date information on a particular topic, please reach out to Vokke via email.

Table of Contents

PIA Methodology

A PIA was conducted during the initial application development. This was prior to the launch of the application and prior to the collection of any personal information. The PIA was conducted by Jon Wellman, Audrey Ahmer and Adrian Grayson-Widarsito (Vokke).

As part of the PIA, all information collected by the system was reviewed and analysed to determine if it was personal and/or sensitive. We determined that personal information (and some sensitive information) will be collected, stored, and used as part of the project. This data may be disclosed by users of the software to other users of the software.

The flow of information through the system was documented thoroughly, both in terms of flow to end-users, and flow through the system architecture. These information flows were reviewed for their adherence to privacy and security best practices - following Australian Privacy Principle (APP) and Open Web Application Security Project (OWASP) guidelines, respectively. During this process, some risks were identified. These risks were then resolved in accordance with the guidelines and the implemented control measures were documented for reference. A Privacy Policy was developed as part of this process and made available to users of the application.

A third party penetration test was then conducted to verify the security of information in the application. Some minor risks were identified during this process, which were then resolved, and verified by a second penetration test.

A detailed PIA was conducted for review by internal stakeholders. This PIA report document was then created and made publicly available alongside the application's Privacy Policy.

Project Description

Research has shown that ADHD patients achieve better outcomes if various symptoms are monitored regularly and treatments are adjusted accordingly, which is currently difficult for clinicians to do. A paper-based worksheet had been developed that makes this process easier. It had been well received by clinicians, however, it is hard to distribute, manage, and scale.

To address these challenges, an online version was developed and made available to clinicians in the community. This web application allows them to record certain information each time they see the patient in order to track their progress over time. The worksheet can be filled in by patients, spouses, caregivers and teachers, when the clinician sends them a link. There is also an admin application, from which AADPA staff can manage clinicians' access to the system.

The application has been commissioned by AADPA in collaboration with Vokke. It has been initially made available to AADPA members, with a wider roll out planned for the future.

The following are stakeholders of the project:

- Jon Wellman (Vokke lead product manager)
- Adrian Grayson-Widarsito (Vokke lead developer)
- Mark Bellgrove (AADPA president)
- David Coghill (Project stakeholder)
- Nicole Stefanac (Project stakeholder)

The PIA has been drafted by Vokke in collaboration with AADPA stakeholders.

Overview of information flows

The following personal information is collected in the system. We note that some of the information regarding Patients is of a sensitive nature (I.e. health information).

- Clinicians
    - First name
    - Surname
    - Email address
    - Organisation
    - Mobile number
- Patients
    - First name
    - Surname
    - Email address
    - Gender
    - Date of birth
    - Post code
    - Parent / Caregiver 1 details (first name, surname, email address, notes)
    - Parent / Caregiver 2 details (first name, surname, email address, notes)
    - Spouse details (first name, surname, email address, notes)
    - Teacher details (first name, surname, email address, notes)
    - Other reporter details (first name, surname, email address, notes)
- Patient clinician visit details
    - Visit date
    - Appointment type
    - Attendees
    - Visit notes
    - Health details
        - Weight / growth (whether it's at an OK level and any notes)
        - Blood pressure (whether it's at an OK level and any notes)
        - Pulse rate
    - Medication details
        - Current medication (primary, secondary, and other medication)
        - Recommended medication (primary, secondary, and other medication)
    - SNAP
    - ASRS
    - Other symptoms
    - CGI
- Non-clinician SNAPs / ASRSs / SKAMPs (symptoms as reported by people other than the clinician)

The diagram below (Figure 1) shows information flow between different users involved in the system. More detail about the information flows can be found in Appendix A.

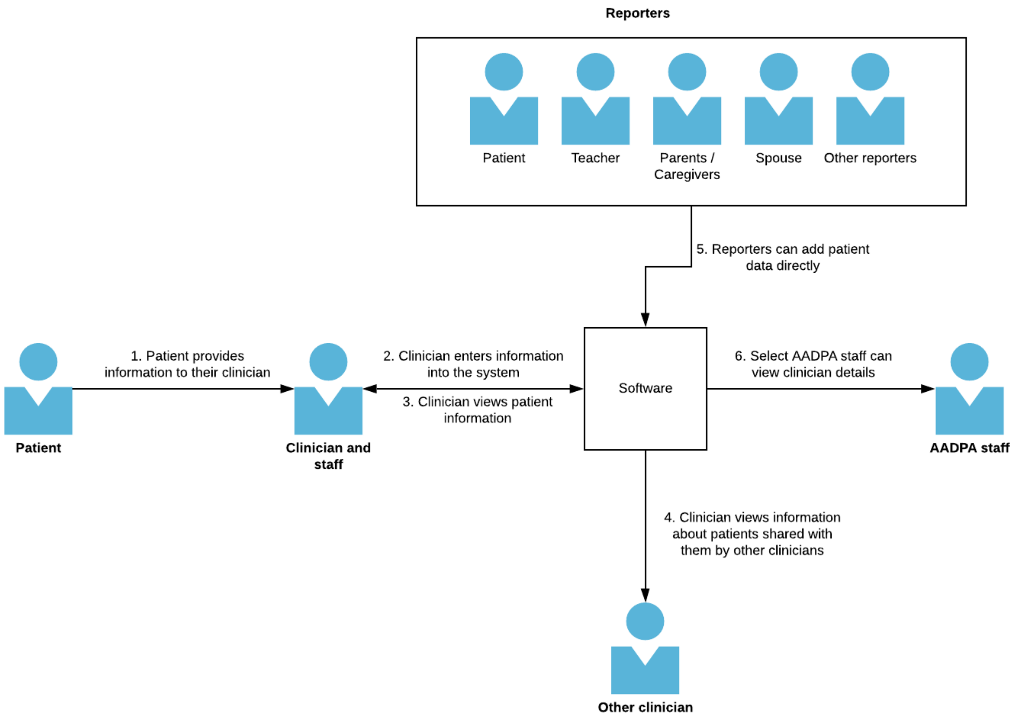
Reporters
Patient
Teacher
Parents / Caregivers
Spouse
Other reporters
5. Reporters can add patient data directly
Patient
1. Patient provides information to their clinician
Clinician and staff
2. Clinician enters information into the system
3. Clinician views patient information
Software
6. Select AADPA staff can view clinician details
AADPA staff
4. Clinician views information about patients shared with them by other clinicians
Other clinician

Figure 1: Overview of information flows in the AADPA software system

System information flows

The diagram below (Figure 2) gives an overview of how information flows within the structure of the system. More detail about these processes may be obtained by contacting Vokke.

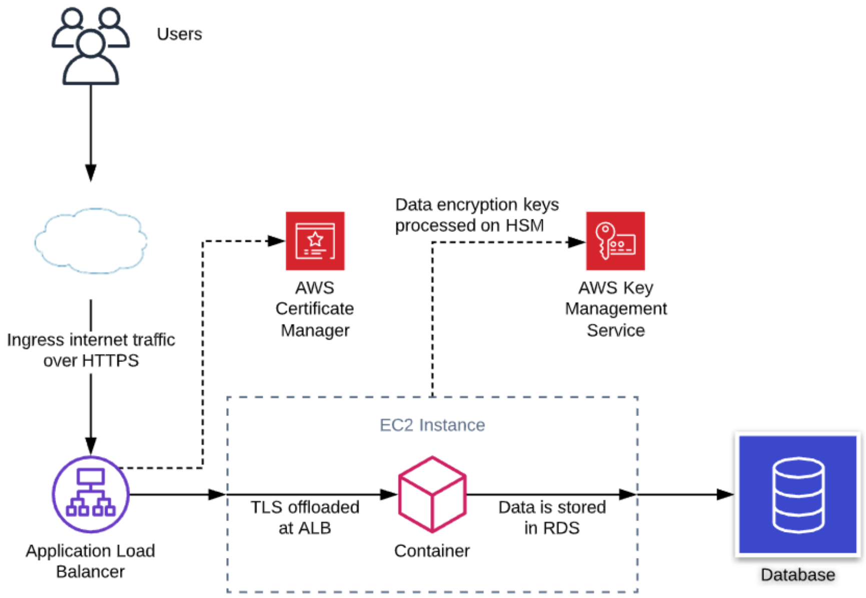
Users
Ingress internet traffic over HTTPS
AWS Certificate Manager
Data encryption keys processed on HSM
AWS Key Management Service
EC2 Instance
Application Load Balancer
TLS offloaded at ALB
Container
Data is stored in RDS
Database

Figure 2: Technical flow of information through the AADPA software system.

Analysis

Privacy impacts of the project

The project has both positive and negative impacts for the privacy of users and patients (Figure 3). We find that, as the system has been designed to replace an existing Clinician process (tracking patient ADHD symptoms), the negative privacy impacts are those that are inherent to the implementation of a software system. These have been mitigated by review and compliance with privacy and security best practices.

Positive privacy impacts	Negative privacy impacts
• Clinicians can manage symptom reports in a secure, encrypted system. Previously, these were gathered in paper checklists which are more easily subject to loss and tampering. • Clinicians are able to easily gather more symptom report from relevant reporters. This ensures that the dataset is as complete and accurate as possible. • Reporters are able to track the patient's condition over time, allowing them to form better judgements about the patients' treatment.	• Patient information will be transmitted online, which is inherently more susceptible to access by unintended/malicious actors than it is within a clinician's physical office. However, we have undertaken an internal audit of security procedures and an external penetration test in order to best identify and minimise any known risks to the security of data in the system. • In the case of a system outage, clinicians and reporters may be temporarily unable to submit reports. This may result in an incomplete dataset.

Figure 3: Privacy impacts of the project

Compliance with APP Guidelines

The project complies with the relevant APPs to the best of our judgement. A review of the application was conducted by Vokke with respect to the APP guidelines. All relevant guidelines and associated risks to privacy were identified and addressed prior to the initial release of the software to production. Details of this review can be viewed in Appendix B. We noted that some privacy principles were not relevant to this project due to the specific nature of the project; I.e. a health-based information system, with a restricted audience of verified health professionals. Vokke and AADPA will continue to review the APPs as new features are added to the system over time.

Some relevant privacy information has been highlighted in the subsections below.

Information quality

When information is displayed in the software it is generally accompanied by the date the information was collected and/or edited. This is to help prevent clinicians using old information. Clinicians are responsible for ensuring that they keep their own data and patient data up to date and accurate.

Security

All patient visit data is encrypted in the database, to protect against unauthorized access of sensitive data.

The system has been implemented and reviewed with reference to OWASP Secure Coding Practices. This process has been undertaken to ensure that authentication mechanisms and access controls are secure and in line with best practices. All identified risks were addressed before the initial release of the software to production.

The system has also been subjected to a third-party penetration test. Some non-critical risks were identified in the penetration test. All identified risks were addressed before the initial release of the software to production.

Retention and destruction

De-identification of information will be performed when AADPA request Vokke to prepare data for Secondary Uses such as research. This will be done programmatically within Vokke’s network perimeter.

Where possible we have developed the web application to remove data from the database rather than simply flag it as archived (so-called *logical deletions*). This data may persist in backups within the backup retention period, after which it will be removed.

Patients and/or clinicians may request that their data be removed from the system. In this case, the requester must identify themselves to the party with whom the data is with respect to.

Access and correction

Clinicians and admin users can access and amend their own data at any time. Patients can provide new information to clinicians who can amend their data on their behalf. This will be handled by clinicians with their patients directly.

Appendix A – Information Flows

The table below details all information captured, stored and distributed through the AADPA software system. Information flow numbers reference the overview of flows (Figure 1).

Information flow	Method	Authentication	Frequency	Required data	Optional data
1. Patient provides information to their clinician	Patients provide information about themselves and their current state to their clinician directly. This may be collected by clinicians however they choose (i.e. it may not be entered into the software directly).	N/A	Information that does not change over time (e.g. patient name) will generally only be provided by the patient once. Information that can change over time and must be monitored (e.g. health details) will usually be provided each time the patient meets with the clinician.	None	First name Surname Email address Gender Date of birth Post code Parent / Caregiver 1 details (first name, surname, email address, notes) Parent / Caregiver 2 details (first name, surname, email address, notes) Teacher details (first name, surname, email address, notes) Other reporter details (first name, surname, email address, notes) Current medication (primary, secondary, and other medication) SNAP (hyperactivity-impulsivity and inattention symptoms) ASRS (adult ADHD symptoms) Other symptoms (details of other symptoms being experienced)
2. Clinician enters information into the system	Clinicians enter data directly into the web software.	Clinicians must have an account and be authenticated prior to entering data for a patient. Clinicians must be approved by an AADPA admin before they can access the system. The clinician must have current access granted (admins can revoke access at any point).	Clinician account data will only be provided when signing up but can be edited by clinicians at any time. Some patient data will be entered when setting up the patient (e.g. name and date of birth). This can be edited at	Clinicians must provide the following personal information to create an account: First name Surname Email address Organisation Mobile number The following personal information	Clinicians can add the following information about the patient: Email address Post code Parent / Caregiver 1 details (first name, surname, email address, notes) Parent / Caregiver 2 details (first name, surname, email address, notes) Teacher details (first name, surname, email address, notes)

		When a clinician first creates their account, they must enable 2-factor authentication. They must utilise 2FA each time they sign in ongoing.	any time as required. Patient data that relates to the patient's current state (e.g. current medication) will be recorded periodically (e.g. each time the patient meets with the clinician).	must be provided to add a patient: First name Surname Gender Date of birth Clinicians can optionally add 'visits'. The only information required to add a visit is the visit date and appointment type.	Other reporter details (first name, surname, email address, notes) Patient clinician visit details Visit date Appointment type Attendees Visit notes Health details Weight / growth (whether it's at a good level and any notes) Blood pressure (whether it's at a good level and any notes) Pulse rate Medication details Current medication (primary, secondary, and other medication) Recommended medication (primary, secondary, and other medication) SNAP (hyperactivity-impulsivity and inattention symptoms) ASRS (Adult ADHD symptoms) Other symptoms (details of other symptoms being experienced) CGI (details of severity of symptoms and improvement since the initial visit) The information that can be collected has been considered and deemed the minimum amount required to achieve the outcomes of the project. It is left up to clinicians to identify patients and verify the information provided. Patients can also be added with a pseudonym if desired.
3. Clinician views patient information	Clinicians view patient data via the web software.	Clinicians must authenticate to view patient data.	This information can be viewed as frequently as required but	N/A	After logging in, clinicians can view all of the information about patients

			will likely be checked periodically when the clinician meets with the patient.		they’ve added to the system and those that other clinicians have shared with them. Clinicians can only view information added by themselves, other clinicians (when a patient is shared), reporters (e.g. parents) and the patient themselves. That is, the system does not attempt to provide additional information about patients (e.g. by integrating with other data sources). The system presents information to the clinician in different forms than how it was entered (e.g. graphs).
4. Clinician views information about patients shared with them by other clinicians	Clinicians can share patient data with other clinicians via the software. If the clinician attempts to share patient data with a clinician that does not yet have an account, the clinician will need to create an account and be approved by an AADPA admin before gaining access. After gaining access to a patient, the clinician can view their data in the web software.	Clinicians must be authenticated and have access to the patient to share them with other clinicians. Other clinicians can only access the shared patient’s data if they’re authenticated and the patient has been shared with them.	Patient data will be shared on an ad hoc basis. Clinicians will view this data on an ad hoc basis.	N/A	Once a clinician has access to a patient that has been shared with them, they can enter data for that patient. This is covered by item 2 above.
5. Reporters can add patient information directly	Clinicians can request information from ‘reporters’ via the software. This includes parents / caregivers, the current teacher, the patient themselves, and other reporters.	Clinicians must be authenticated to request data from a reporter for a patient. They can only request this for patients they have access to. Reporters can only provide information about	Requests will be sent to reporters on an ad hoc basis (e.g. each time the clinician is going to meet with the patient).	N/A	The web form contains a list of inattention and hyperactivity-impulsivity symptoms and prompts the reporter to provide a score for each one based on their observations.

	Requests will be sent to reporters via email and will contain no personal information other than the patient's name. The email will contain a URL to a web form that the reporter can use to provide information about the patient. The URL is uniquely generated for the specific request, patient, and reporter. The web form does not display any personal information about the patient or any other patients.	a patient if a clinician has sent them a request. That is, the system does not support reporters entering unrequested information at will. As a means of authentication, Reporters must correctly identify the patient's DOB in order to submit the report.			Providing information via this process is entirely optional, however, reporters must provide a full set of information if they decide to provide any at all.
6. Select AADPA staff can view clinician details	Certain AADPA staff will have access to an administration portal. This provides the staff member with functionality to administer and approve clinician accounts. Administrators will have different access permissions to Clinicians in the portal.	Admin users must authenticate to view any data or perform any actions. AADPA staff can be provided with access to the administration portal by other admin users. The first time a new admin user access the system, they must set up 2-factor authentication. They must utilize 2FA each time they sign in ongoing. Admin users can prevent clinicians from accessing the system at any time.	Information will be viewed on an ad hoc basis.	N/A	Patient data can't be accessed from this application. Admin users can only view basic clinician data (e.g. name and organisation).

Appendix B – APP Guidelines Checklist

APP #	Guideline	Further notes from APP	Relevant	Describe how the guideline is/will be met, or the compensating control
APP 1 - Open and transparent management of personal information				
1.3; 1.4	Have a clearly expressed and up-to-date APP Privacy Policy about how the entity manages personal information	Requires regular review Make available free of charge in appropriate form	Yes	A Privacy Policy has been developed and adopted by AADPA. This is available for clinicians to view when signing up to the site. This will be reviewed upon any changes to the application that affect privacy.
1.7	Conduct a Privacy Impact Assessment (PIA) for new projects in which personal information will be handled, or when a change is proposed to information handling practices		Yes	A PIA has been collaboratively developed by Vokke and AADPA. A public-facing PIA report will be accessible from the Privacy Policy.
1.7	Implement and evaluate security systems for protecting personal information from misuse, interference and loss and from unauthorised access, modification or disclosure		Yes	A comprehensive security audit has been conducted, with reference to OWASP guidelines (see Appendix A). The application has also been subject to an external penetration test.
1.7	Establish procedures for identifying and responding to privacy breaches, handling access and correction requests and receiving and responding to complaints and inquiries		Yes	Procedure established and agreed upon between Vokke and AADPA. This will be documented in the Privacy policy along with contact details for making such a request/complaint. Vokke staff will receive training on the Notifiable Data Breach scheme.
1.7	Establish mechanisms to ensure that agents and contractors in the service of, or acting on behalf of, the entity comply with the APPs		Yes	Vokke must comply with APPs. Clinicians must comply with APPs – this will be a guided process throughout the application, in which clinicians agree to privacy terms and check that they have obtained patient consent for each relevant action.
1.22	Establish a generic telephone number		Yes	Vokke can be contacted at privacy@vokke.com.au

	and email address that will not change with staff movements (for example privacy@agency.gov.au)			AADPA can be contacted at admin@aadpa.com.au
APP 2 - Anonymity and pseudonymity				
2.1	Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter	Not relevant if impracticable for entity to deal with individuals who have not identified themselves	Partially	In the application, it is impractical to have individuals anonymous/pseudonymous. Support requests may be handled anonymously, depending on the circumstances.
2.16	If an APP entity is 'required' by a law or order to deal only with an identified individual it will be necessary for the individual to provide adequate identification. If an entity is 'authorised' by a law or order to deal with an identified individual, the entity can require the individual to identify themselves, but equally will have discretion to allow the individual to deal with the entity anonymously or pseudonymously.		No	-
2.22	An APP entity that is relying on APP 2.2(b) (impractablity clause) should not collect more personal information than is required to facilitate the dealing with an individual		Yes	This has been considered. Minimal personal information about Clinicians and Patients is collected.

APP 3 - Collection of solicited personal information				
3.1	only solicit and collect personal information that is reasonably necessary for one or more of its functions or activities		Yes	This has been considered. Minimal personal information about Clinicians and Patients is collected.
3.3	only solicit and collect sensitive information if the individual consents to the sensitive information being collected		Yes	Health data is sensitive. Clinicians must indicate within the app that they have obtained patient's (or caregiver's) consent to data being stored, when adding a new patient or a new visit. Consent should be obtained to use personal information (not sensitive) for secondary purposes (analytics, logs).
3.3	solicit and collect personal information only by lawful and fair means		Yes	This has been met. All data is provided by either clinicians or specified reporters.
3.3	solicit and collect personal information directly from the individual, unless exception applies	Exceptions include unreasonability/impracticability of collecting only from individual	Yes	The SNAP/ASRS/SKAMP questionnaires are filled out about the patient, by other parties. Other information is entered by Clinician with reference to the patient. This is the purpose of the application, so it is therefore necessary in this case, and unreasonable/impracticable to do otherwise. A checkbox had been added to confirm patient consent on sending the forms to reporters.
3.22	the individual about whom the sensitive information relates must consent to the collection	Permitted if providing a health service and collecting information in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation	Yes	Clinicians will be bound by established professional confidentiality agreements.
APP 4 - Dealing with unsolicited personal information				
	If an APP entity receives unsolicited personal information, it must decide whether it could have		No	The app never collects/stores unsolicited information

	collected the information under APP 3			
	If the entity determines it could not have collected the personal information under APP 3, different rules apply according to whether or not the information is contained in a 'Commonwealth record'.		No	-
	If the unsolicited personal information is contained in a Commonwealth record, APP 4 does not require it to be destroyed or de-identified.		No	-
	Other unsolicited personal information that could not have been collected under APP 3, must be destroyed or de-identified as soon as practicable if it is lawful and reasonable to do so.		No	-
	If an APP entity is not required to destroy or de-identify the unsolicited personal information under APP 4, the entity may retain the personal information but must deal with it in accordance with APPs 5–13.		No	-
APP 5 - Notification of the collection of personal information				
5.1	take reasonable steps either to notify the individual about personal information collected or to ensure	at or before the time an APP entity collects an individual's personal information, or if that is not practicable, as soon as	Partially	Clinician is informed to notify patient about data collection (on adding the patient, adding visits and sending report forms). The patient is not contacted directly by the system.

	the individual is aware of those matters	practicable after the collection occurs		
APP 6 - Use or disclosure of personal information				
6.1	only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies.		Yes	This is met within the app - primary purpose is clinicians managing patients. Sensitive data will not be used for secondary purposes such as analytics, logs, admin panels.
6.72	take reasonable steps to ensure that health information is de-identified, before it discloses the information		Yes	Information will be de-identified by Vokke if it is requested by AADPA for disclosure. Patients will not be identified in secondary systems (eg analytics). Patient identity must be maintained when their records are shared with another clinician. This will only be upon consent from the patient and at the discretion of the original clinician.
APP 7 - Direct marketing				
7.1	Do not use or disclose personal information it holds for the purpose of direct marketing unless an exception applies	This can depend on where the data was sourced from, and whether or not the individual would reasonably expect their personal information to be used for the purpose of direct marketing	No	Personal information held in the application will not be used for marketing purposes.
7.3	provide a simple means by which an individual can request not to receive direct marketing communications	The organisation must give effect to any such request by an individual within a reasonable period of time and for free	No	-
7.7	An organisation must, on request, notify an individual of its source of the individual's personal information that it has used or disclosed for the purpose of direct marketing unless this		No	-

	is unreasonable or impracticable to do so			
APP 8 - Cross-border disclosure of personal information				
8.2	Before an APP entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information		Partially	Clinicians will be AADPA members / practicing in Australia or New Zealand. Clinicians will be able to add their patient records into the system and view their own records. Clinicians must agree to the Privacy Policy and Terms of Use upon registering an account, as well as prompts for consent while using the application. Information in the system is not intended to be disclosed to any other overseas recipients.
APP 9 - Adoption, use or disclosure of government related identifiers				
9.1	An organisation must not adopt, use or disclose a government related identifier unless an exception applies.	The objective of APP 9 is to restrict general use of government related identifiers by organisations so that they do not become universal identifiers. That could jeopardise privacy by enabling personal information from different sources to be matched and linked in ways that an individual may not agree with or expect. - excludes name and ABN	No	This is currently met. This should also be considered for future requirements – eg. Unable to store medicare number
APP 10 - Quality of personal information				
10.1	take reasonable steps to ensure that the personal information collected is accurate, up-to-date and complete		Partially	Health data will be historical with respect to the time of collection (eg patient's appointment) and so do not need to maintain one authoritative state. Contact details should be up-to-date, accurate and complete for the purpose of use, but this will not affect the quality of health data.
10.2	take reasonable steps to ensure that the		No	We trust that clinicians will use the historical data appropriately. However, we

	personal information it uses and discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.			will: - Ensure that historical data is displayed with respect to date. - Implement a 'date last edited' field. -Ensure that graphs clearly display the frequency of SNAP/SKAMP reports so that Clinicians can keep data up to date -Allow clinicians to mark patients as active/inactive to set expectations for accuracy of records.
10.16	Personal information held by an APP entity that is no longer needed for any purpose, may need to be destroyed or de-identified		Yes	Patient records will be kept by default, as they preserve a record of health information. Clinicians may mark patient(s) as inactive for their own record-keeping, which hides them from easy access. Information may be de-identified by Vokke upon request; the requesting party must identify themselves to be the subject of the personal information.
APP 11 - Security of personal information				
11.2	take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure	Reasonable steps include: • governance, culture and training • internal practices, procedures and systems • ICT security • access security • third party providers (including cloud computing) • data breaches • physical security • destruction and de-identification • standards	Yes	Considered when conducting the PIA, during audit of software security, as well as implementation of OWASP security guidelines. Including the following outcomes: - Set up a WAF with ModSecurity - Set up Australian logging service via CloudWatch - Encryption of sensitive block data (visit information)
11.3	take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for any purpose for which the personal information may be used or disclosed		Yes	Addressed in a guideline above. Personal information may be de-identified upon request.

APP 12 - Access to personal information				
12.1	entity that holds personal information about an individual must, on request, give that individual access to the information	There are exceptions to this, and some cases where access must be refused (refers to other acts, eg FOI act)	Partially	Functionality has been added to export patient data to PDF. Patients/caregivers may request this from clinicians. It is at the clinician’s discretion to grant access to this.
12.2	a written notice, including the reasons for the refusal, must be given to the individual if access is refused		Partially	As above
12.15	entity must be satisfied that a request for personal information under APP 12 is made by the individual concerned, or by another person who is authorised to make a request on their behalf, for example, as a legal guardian or authorised agent.	The minimum amount of personal information needed to establish an individual’s identity should be sought	Partially	As above. A checkbox has been added to the export functionality to confirm that data will be given to the individual concerned.
APP 13 - Correction of personal information				
13.1	take reasonable steps to correct personal information it holds, to ensure it is accurate, up-to-date, complete, relevant and not misleading, having regard to the purpose for which it is held		Partially	This will be for clinicians to manage their records. Functionality to edit visits has been implemented to facilitate this.
13.4	upon request by an individual whose personal information has been corrected, take reasonable steps to notify another APP entity of a correction made to personal information that was previously provided to that other entity		No	Information not disclosed to other entities.

13.21	Privacy Policy contains information about how the individual may seek correction of their personal information held by the entity		Yes	Added to Privacy Policy.