Med App Data Protection Impact Assessment

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Project Aims: Med App brings relevant information to clinicians fingertips to enable staff wellbeing and safe patient care. We Create a seamlessly connected Australian (and global) network of clinicians, where the information for how they do their job is at their fingertips, they are onboarded and orientated effectively, it is linked with their educational and professional attainments, allowing easy tracking of their own performance towards their various career goals, as well as facilitating moving between different sites.

Processing Activities: Below are the core pieces of data and processing activities conducted by using the platform. Some data may or may not be processed depending on the feature set used by customer sites.

- Registration Information includes Email, Phone number, First name and Last name.
    - This information is used to confirm a user is a real person and ensure duplicate user profiles are not entered into the system. It also allows for password resets and sending of critical information to the user from their hospital (via SMS if using Mailouts).
    - This information is also used to contact users if they request technical support through our help centre or we are required to communicate data breaches or critical changes that affect them.
- Usage Data. Anonymised and non-anonymised usage data is collected through the application.
    - Anonymised data for mobile users. This includes sessions, number of screen views, session time and interactions across the app. It also includes logging information for error and bug identification. Aggregated, anonymised data is shared with customer sites (their own data) to guide them in content and communication improvements and in assessing value. Med App also uses this aggregated data to measure feature performance and improve the experience for users.
    - Non-anonymised for dashboard users. This is used alongside the anonymised data to ensure dashboard users are maintaining appropriate governance and allows customer hospitals to monitor content uploads, changes and communications. This is required to ensure appropriate organisational and clinical governance is maintained at all times.

- Forms Data (optional). Various assessment related information (customised based on forms)
    - If a customer hospital is using the Forms feature they may have it setup to collect information relating to the users based on templated forms. The information to be collected is determined by the individual hospital. Med App will provide the collection and processing of that information. That information will be available to the everyone involved in the forms workflow (e.g. clinician, assessor, administrator). As an official form the information may not be edited after it is completed and signed, unless the form is reset for administrative purposes.

Need for DPIA: As part of best practice and for compliance with GDPR we identified the need to complete the DPIA.

Step 2: Describe the processing

Describe the nature of the processing: *how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?*

Data Collection:

- Users can register their own details in the platform or complete forms available to them in the app.
- Customer hospitals may send invites to users employed at their site. This information is collected as part of the users employment.

Data Use:

- Verify real users
- Allow them to reset passwords and retrieve login details
- Provide technical support and success services
- Allow them to digitally complete forms for their clinical practice and employment
- Anonymised, aggregated usage analytics and benchmarking for hospitals and application improvement

Data Storage:

- Data is stored in line with our existing Encryption Policy and our Data Retention Policy

Data Deletion:

- Data is deleted in line with our existing Data Retention Policy.

Data Source:

- Individual users
- Hospital employers of the users

Data Sharing:

- No data is shared with other accounts on Med App (a user may still be invited to another hospital, or request access to another account if they move hospital).
- Data may be shared to sub-processors used for cloud servers/storage, authentication providers and providing technical support communication.

High Risk Processing:

- No high risk processing has been identified.

Describe the scope of the processing: *what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?*

Nature of Data:

- Registration Data. User identification data (names, email, phone number).
- Form data. This will vary customer site to customer site depending on they type of forms, assessments or HR forms set up. This will relate to the clinicians employment with their hospital or their professional accreditation requirements.
- Usage data. Anonymised, aggregated data from usage of the platform.

Special Category or Criminal Offence Data:

- No

Amount of Data Collection:

- Currently registration data has been collected for approximately 44,000 users
- Forms data has been collected for approximately 1,000 users.
- Analytics will vary depending on use, currently this is at 5,000 active users p/month.

Frequency of Data Collection:

- Registration data is collected once on registration (or invitation).
- Forms data may be collected at varying intervals (e.g. 2 times per clinical term, or 30 times over 12 months).
- Usage data is collected on a real time, ongoing basis.

Data Retention:

- Data is retained in line with the current Data Retention Policy.
- Registration data will be retained as long as a user has an account in Med App. If an account is deleted, backups containing this information will be superseded after 30 days.
- Usage analytics data will be held for an indefinite period.

Affected Individuals:

- Total registered users in Med App is approximately 44,000 users.

Geographic Area:

- Med App is primarily used in Australia and New Zealand. We do have smaller implementation in the UK and upcoming implementations in Ireland.

Describe the context of the processing: *what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor*

in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Relationship with Users:

- Users may freely register themselves in Med App.
- Users may be invited or approved for access in Med App by their employer hospital or health facility. In this situation we will provide access to the customer account, in addition to the freely available 'Open Access Med App' account.
- We do not charge the end users fees for using or registering in the account.
- Hospitals are the ultimate customers and pay a subscription to operate an account within Med App. Through this they are given dashboard access which allows them to control the content, communications in the account and users who have access to it.

User Control of Data:

- Users have full control over the personal information that is registered in the app. They are able to update it at any time as well as delete their account directly via the app.
- Customers dashboard managers are able to manage all content, communications and user access via the designated dashboard.
- Some data users submit via forms relates to their professional and hospital accreditation. This data will be retained by the hospital and may be submitted to regulatory authorities as is required.

Data Use Expectations:

- We expect that users and customers would expect Med App to use data in the ways outlined. This inline with the customer contracts and the Med App privacy policy.

Children or Vulnerable Groups:

- Med App does not collect data from children or vulnerable groups.

Processing Concerns or Security Flaws:

- There are no concerns over the processing of this information and no known security flaws in the processing, storage or encryption of the information.
- This will be reviewed and updated at least annually, but also on a project by project basis.

Novel Processing:

- No novel processing is present.

State of Technology:

- Med App is using industry standard technology and sub processors for the processing of data. Registration data, forms data and usage analytics are all mainstream data that is handled in line with current security and privacy standards.

Relevant Current Issues of Public Concerns:

- In light of recent data breaches there is increasing concern about the type of data being held by companies, where it is stored and the level of security that exists to protect it.
- Recent data breaches in the health sector further highlight this.
- Ransomware attacks on hospitals in Australia over the last 5 years also increase the need for healthcare organisations to maintain high level security internally and with suppliers.

Applicable Codes of Conduct:

- While not required to, Med App complies with the Australian Privacy Principles and relevant privacy legislation in Australia.

Describe the purposes of the processing: *what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?*

Goals for Data Processing:

- Maintain security of the platform for the benefit of the users on the platform.
- Ensure data is accurate.
- Allow for clinicians to interact efficiently with hospital information and relevant communications, removing paper and streamlining complex workflows.
- Measure the effectiveness of implementations and value for customer facilities.

Effect of Processing on Users:

- The objective of processing the data is to improve the working experience of clinicians in hospitals and related healthcare facilities.
- No potential or current impact has been identified that would effect users as a result of processing data.

Benefits of Processing:

- The benefits outlined above are a more efficient interaction with hospital administration and education. Better access to relevant information and communications that are essential for clinicians doing their job in hospitals and providing easier access to wellbeing resources and information.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: *describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?*

Process for Stakeholder Consultation:

- Med App has consulted mobile users (clinicians) and dashboard users through the process of development.
- We also conduct ongoing engagement and feedback sessions with clinicians which include collecting feedback on privacy and security concerns for users and data.

Additional Processor Involvement:

- Not required at this time.

Information Security Expert Consultation:

- Med App has engaged the Drata information security mapping tool to assist in monitoring and maintaining compliance with the ISO27001 standard.
- Med App will engage additional information security professionals as needed.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: *what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?*

Lawful Basis for Processing:

- Legitimate interest (Article 6(1)(f) GDPR)

Processing in Relation to Purpose:

- Processing of the data in its current form is achieving our purpose.

Other Ways to Achieve Outcome:

- No alternative ways to achieve Med App's purpose or the current outcome have been identified.

Function Creep:

- We conduct an analysis of required data and continue to anonymise and aggregate usage data.
- We ensure that we live up to Med Apps core values, vision and mission and all our projects are developed in accordance with those principles..

Data Quality:

- Users have full access to their own data which can be updated directly through the mobile app.
- Forms data is locked as static content once it has been signed off to prevent unauthorised edits. Further we also provide a change log with each form completion to assist people in verifying the history and authenticity of that document.

Data Minimisation:

- Med App aims to collect only the data that is absolutely necessary to give a seamless user experience. Registration data is minimised and usage data is anonymised and aggregated for benchmarking purposes.

Information for Users:

- Information is available though our privacy policy, as well as our company blogs. Where we receive user requests for information we are more than happy to provide additional information via email or through the live chat.

Support of User Rights:

- We will make every effort to comply with privacy and security legislation and further, live up to the standards expected of technology companies by the community, and specifically the healthcare community.

Measures for Processor Compliance:

- Med App data processors are selected for their performance and compliance with security and privacy requirements. We ensure relevant data processing agreements are in place and review these annually to ensure they continue to meet industry and community standards.

International Transfer Safeguards:

- Med App ensures data is stored and processed onshore in Australia. We do not currently allow for selection of processing regions within customer accounts.

Step 5: Identify and assess risks

See the company risk register which contains relevant risk assessments in relation to security, privacy and data processing.

Step 6: Identify measures to reduce risk

See the company risk register which contains relevant risk assessments in relation to security, privacy and data processing.

Step 7: Sign off and record outcomes

Item	Name/Date	Notes
Measures approved by:	Duncan Paradice	Post project review of privacy and security of data in Med App core platform.
Residual risks approved by:	See company risk register in Drata	If accepting any residual high risk, consult MA management team.
DPO advice provided:	Not applicable at this time	
Summary of DPO advice: Not applicable at this time		
DPO advice accepted or overruled by: Not applicable at this time		
Comments:		
Consultation responses reviewed by:		

Comments:		
This DPIA will kept under review by:	Duncan Paradice	To be reviewed annually, next on 30 June 2025