Airmid Privacy Policy

Updated on 04/11/2020.

The Phoenix Partnership (Leeds) Ltd ("TPP") have developed Airmid (the "App") to provide you with access to and the ability to contribute to your own health and care record from your smartphone or other personal device.

TPP is committed to protecting and respecting your privacy.

To provide the App and associated services, we must process information about you. Please read the following carefully to understand our practices regarding your personal data and how we will treat it.

This policy (together with the End User Licence Agreement for the App) sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us. By creating a user account on or using the App you are accepting and consenting to this policy.

1. Personal information

The following information is used by us in order to provide the App and services:

Information you give us

You may provide us with information through your use of the App, including Personal Data and Special Categories of Personal Data. This includes:

- *personal information* that we ask for in order for you to create an account (such as your name, gender, date of birth, ID number and phone number/email address) to access the App;
- *medical and lifestyle information* which contains sensitive personal information contained within your medical record. This information has been recorded by organisations who are/have been caring for you and who have allowed you to view the record they hold within the App. You consent for this data to be shared to and made visible in the App by your use of it and acceptance of this policy;
- *demographic, medical and lifestyle information* that you add to the App or your medical record;
- *information in or about the content you provide* (e.g. metadata), such as the date and time when information is added.

Information we collect about you:

We may collect information from your use of the App and our services, including:

- *Device and Connection information,* such as the type of device, operating system, mobile network information and phone number; Connection information such as the name of your mobile operator or ISP, browser type, language and time zone, mobile phone number and IP address;
- *Usage Information and automatic activity tracking*, such as how and when you use the service and what content and functionality you access;
- *Location information*, including specific geographic locations, such as through GPS, Bluetooth, or WiFi signals, when location services settings are activated;
- *Information from partner apps and apps that use the App/services,* such as information collected by us when you visit or use third-party apps and apps that use the App and/or our services;
- *Information about transactions made on the App.* If you use the App for purchases or other financial transactions, we may collect information about the purchase or transaction.

NHS login:

Please note that if you use your NHS login details to access the App, the NHS login identity verification services are managed by NHS Digital. NHS Digital is the controller for any personal information you provided to NHS Digital to create your NHS login account and verify your identity, and uses that personal information solely for that purpose. For that personal information, our role is a processor only and we must act under the instructions provided by NHS Digital (as the controller) when verifying your identity. Tap here to see NHS Digital's Privacy Notice and Terms and Conditions. This restriction does not apply to the personal information you provide to us separately.

2. Uses of personal information

We use the personal information that we collect (subject to choices you make) for the following purposes:

- *To provide our services and to suggest products, including to personalise features and content, services or additional functionality that you may find helpful.* In order to create a personalised app and services that are unique and relevant to you, we use:
  - Information on how you use and interact with the App and services;
  - Location-related information – such as your current location, where you live, the places you like to go, and the locations, organisations and people you're near (location-related information can be based on things such as precise device location (if you've allowed us to collect it), IP addresses and information from your use of the App).
- *To improve our services and to ensure that content is presented in the most effective manner* for you and for your device. We use the information we have to send you communications and to respond to you when you contact us.
- *To allow you to participate in the interactive features of our services*, when you choose to do so.
- *To help us keep the App safe and secure*. We use the information that we have to verify accounts and activity, combat harmful conduct, detect and prevent bad experiences, maintain the integrity of the App and services, and promote safety and security on and off the App. For example, we use data that we have to investigate suspicious activity or breaches the Airmid Terms of Use.

3. Non-personal information

We also collect anonymised data in a form that does not allow identification of you:

- *To monitor usage and collect usage statistics for product research and development* including but not limited to how the App services are being used. We use the information to develop, test and improve the App and services, including by means of conducting surveys and research, and testing and troubleshooting for existing and new products and features.

4. How your data is shared

The App enables you to:

- create your own medical/health record in the App, for example, recording any allergies and sensitivities that you have; and
- view your health and/or care record (or elements of it) created and controlled by organisations that provide health and care services to you (if they choose to make

this available to you through the App), for example information your GP writes into your electronic medical record to note what has happened to you, information your hospital creates when you attend, information the district nurse keeps of care you receive, etc.

Sharing with organisations involved in your care: To view your health and/or care record created by others (such as your GP, your community nurse, a hospital you have visited etc.) via the App:

- The organisation(s) that care for you will need to allow the record that they hold about you to be made visible to you via the App. You will not be able to see parts of your medical record on the App if the particular organisation(s) that hold that information have not allowed you to do so. For example, your GP can switch on the ability for you to see your GP record, and any other care provider who is using TPP's SystmOne electronic record software or Emis Health Limited's electronic patient record software can also choose to share information they have saved to your record with you; and
- You will have already consented to providing this information to the App by agreeing to the Airmid Terms of Use (including End User Licence Agreement) and this Privacy Policy;

To allow an organisation to see the data that you record on the App:

- You will need to consent to the data that you record being shared to that organisation and turn on the switch to do so in the App via the Organisations screen;
- The organisation will need to consent to see the data that you recorded by turning on the switch to do so in the SystmOne electronic patient record software.

This is done per organisation that provides health or care services to you. You can amend your consent to share with these organisations from the Organisations screen.

Once an organisation is able to see the data you record via the App and you have subscribed to receive information from that organisation they are able to choose to incorporate data you record via the App into their medical record about you (which may then be shared by them with other organisations involved in your care) but this is only where:

- The organisation has requested the data from you. For example, via a questionnaire or template.

Should this happen there will be some implications in terms of data retention and deletion – see the Airmid Deletion Policy.

Family access:

If Family access (where somebody has access to another person's record through the App) is granted on a legal basis (e.g. parental responsibility for a child), the proxy user will automatically be granted access to view, add to, edit and remove that person's App data. For example, if you are granted Family access you would be able to view and record information on your child's record, or, with their consent, your parent's record.

If you do become a proxy user the person whose record is being accessed will see within the App that your proxy access has been granted on a legal basis. In the same way, if someone has proxy access to your record, you will be able to see this within the App.

Sharing with researchers:

You are able to give us consent to disclose your personal information to selected other third parties via the App as part of the service. For example you may want to help a project being undertaken by researchers who are working to improve health and care provision for the benefit of you and the public. You will be asked if you want to share your information with these other parties. The details of this are in the Help the NHS section and you will have to specifically opt-in to share your personal data in this way. To be clear, you can use the App without opting in to share your data with researchers.

Because of our responsibilities to you, we will only disclose or share your personal data in the following circumstances:

- When you have given us consent as described above; or
- If we have a legal obligation to do so; or
- If it is necessary to comply with a request from a public or governmental organisation.

An example of a legal obligation would be if a court ordered us to disclose information; in a similar way the government can issue orders that require information to be shared.

If our ownership or control of all or part of our services transfers to a new owner, we may transfer your personal information to the new owner. If this happens, the new owner will be obligated to continue to treat such personal data on the terms set out in this Privacy Policy and inform you of their ownership.

5. Our legal basis for processing data

We act as data controller for data that you enter into the app

We collect, use and share data that we have access to (as described above):

- To fulfil our Terms of Use;
- To comply with our legal obligations;
- To ensure we respect your consent, which you may revoke at any time through the App;
- To protect your interest, or those of others;
- As necessary in the public interest;
- As necessary for our (or others') legitimate interests, including our interests in providing an innovative, personalised, safe and profitable service to our users and partners, unless those interests are overridden by your interests or fundamental rights and freedoms that require protection of personal data.

6. Data Retention

We retain data until it is no longer necessary for the provision of the App or delivery of our services, or until you request that your App account is deleted. Where no activity has taken place within the app we will retain the data for a maximum period of 21 years from the date of last activity. This period allows for an individual using the App who is deemed Gillick competent at the age of 12 to attain the age of majority and have available the maximum period to seek redress in a court (6 + 15 years). This extended period also provides an extended but not unlimited period for those without capacity.

7. Your Rights

You have specific rights under the Data Protection Act 2018 and the GDPR.

Data you enter

The App provides you with control over the data you enter on the App. You can:

- *Access your personal information* except in exceptional cases provided for by laws and regulations. You may access your personal information by logging into the App. Sometimes you may also need to contact the relevant health or care provider who holds your record;
- *Correct or supplement your personal information.*

If you find an error in the personal information you have created that we process, you have the right to ask TPP to make corrections or additions if you are unable to correct it yourself in the App. Where the incorrect information is coming from one of your health or care providers you will need to ask them to make the correction.

Changing your consent to share data

You can choose which organisations can access the data you enter on the App. You do this by consenting to share your data with specific organisations from within the App settings. You can revoke this consent at any time.

Please be aware that whether the organisations can access your data is subject to conditions described in section 4 of this Privacy Policy.

When you withdraw your consent to share data with an organisation, that organisation will no longer be able to view any data you enter (or have previously entered) via the App.

Data that you provide for research is handled differently. See the 'Research Data' section in the Airmid Deletion Policy for details.

Requests for deletion and removal of your personal information

As stated above you may request the removal and/or deletion of your personal information – please see our Deletion Policy for more information on how to do this and what this means.

8. Information security and preventing harm

We make it a priority to provide strong security and give you confidence that your information is safe and accessible when you need it. The App is built with strong security features that continuously protect your information. We use strict procedures and employ strict security features in accordance with industry best practice and standards. We take all steps reasonably necessary to ensure that we treat your data securely and in accordance with this Privacy Policy.

We restrict access to your personal information strictly to TPP employees, contractors, and agents who need access in order to process it. Anyone with this access is subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.

In addition to this, it is your responsibility to ensure your computer or device, and your connection to the service, is secure. Use of the App and our services is at your own risk. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to us via any device on which you may access the App.

9. Use of App services by a person under 16

We will only permit a person under 16 to use the App (and in so doing collect and use sensitive their personal data) if they are deemed to be Gillick competent by a responsible professional. Gillick competence is a term originating in English Law to decide if a person under 16 years of age is able to consent to their own medical treatment without the need for parental permission or knowledge.

10. Changes to this policy

We may need to change this Privacy Policy to reflect changes in law or best practice, to deal with additional features or changes to features that we introduce or to apply other updates.

When any updates are made to this Privacy Policy, we will notify you when you next start the App. If you do not accept the notified changes, you will not be permitted to continue to use the App.

If you continue to use the App following notice of the changes to the Privacy Policy, it constitutes your acceptance of the updates.

11. How we operate and transfer data as part of our global services

We share information internally within TPP, externally with our partners and with selected organisations for research purposes (subject to you providing consent to do so) and with those you connect and share with around the world in accordance with this Privacy Policy. Information will be transferred or transmitted to, or stored and processed in the United Kingdom or other countries outside where you live for the purposes as described in this Policy but always securely and in accordance with data protection law.

12. How to contact TPP with questions

If you have general questions or comments about the App, you can email us at: AppEnquiries@tpp-uk.com

If you have questions about this Privacy Policy, you can contact TPP's Data Protection Officer at: dpo@tpp-uk.com

Airmid Deletion Policy

In this policy, any references to data ‘deletion’ mean data being ‘put beyond use’, a process that is recognised by the Information Commissioner’s Office (ICO) as a form of data deletion. Please see the ‘Beyond Use’ section at the end of this Deletion Policy for more details.

We, TPP, have developed Airmid (the “App”) to provide you with access to and the ability to contribute to your health and care record from your smartphone or other personal device. We also provide you with the ability to support research into health and care. We act as the data controller for data entered by you in the App. For more information about our services and our role and responsibilities please see the End User License Agreement (EULA).

This Deletion Policy explains how data can be removed or deleted from the App. We process all requests for deletion in accordance with the GDPR and the Data Protection Act 2018, and with guidance provided by the Information Commissioner’s Office. Personal information is retained by us until it is no longer necessary for the provision of the App or our services to you, or until you request its deletion (whichever comes first).

Data Removal

Within the App you can remove individual data items that you have entered via the App at any time. These items will no longer be visible to you within the App but will still visible to the organisations that you share data with, but clearly marked as having been marked as removed by you.You are not able to remove or change data recorded by your health or care provider using the App. This includes any data items which your health and/or care provider(s) have chosen to incorporate into the medical record they hold about you, You should contact your health or care provider directly to request deletion or amendment of data items within your record added by a health or care professional.

Account Deactivation

You can also choose to disable your App account at any time. This will make the data you have entered inaccessible to anyone, including those organisations you have previously shared data with, unless you reactivate your account.

You can disable your App account in the App via your App Profile. Once you disable your App account, your health and care providers or third parties with whom you have previously consented to share your data will no longer be able to access the data you have entered via the App.

Any data you have entered via the App that has been subsequently incorporated into a record held by an organisation involved in your care will remain visible in that record about you - for example, information that has been requested by an organisation via a questionnaire or template.

Any data you have added to other patient records using proxy access will still be accessible to their health and care providers, unless they disable their own account.

Disabling the App does *not* delete the data you have entered into your record. Your data will be securely retained so that it is available if you want to reactivate your account in the future.

If you reactivate your App account (and agree to our Terms of Use (including End User Licence Agreement), Privacy Policy and End User Licence Agreement), your health or care provider will be able to access the data you record via the App and have consented to share with them. This includes the data you previously recorded before disabling your account.

Data Deletion

We recognise there are certain circumstances where you may request that we delete your data in accordance with the below principles. These are listed below:

- If we deal with your personal information in violation of laws and regulations;

- If our handling of your personal information is a serious breach of our agreement with you;
- If you no longer use the App or our services, or you disable your App account;
- If we permanently no longer provide you with products or services.

You can delete the data you have entered into your own record yourself from within the App. You can do this by selecting the '*Permanently delete data that I have added to my medical record*' option when disabling your App account. The data will be securely deleted in accordance with the 'Deletion Principles' below;

Deletion Principles

1. By requesting data that you have entered into the App to be deleted, you understand this will mean that the data will no longer be accessible, including by yourself.
2. The data in scope for deletion is personal data entered by you and associated metadata.
3. The data outside the scope for deletion is;
    a. Data that you have consented to sharing with research organisations through the App;
    b. Data created by health or care organisations that is visible to you in the App; and
    c. Data you have added via the App in response to a request from a health or care provider, such as information requested within a questionnaire or template.
4. Any in-scope data will be deleted by it being put beyond use.
5. Any requests for deletion of out-of-scope data will need to be raised with either the specific research organisation or the health or care provider who holds your medical record.
6. If you delete data directly through the App, this deletion will happen immediately. If you email us to request deletion of proxy ('Family') access data, we will assess the request and process it in a timely manner – see Proxy access data below.
7. Following deletion, we will no longer be able to assist you with access to such data and all processing activities by us shall cease.
8. We will not charge a fee for reasonable deletion requests but may charge a fee for repeated requests that exceed reasonable limits, as appropriate.

Beyond Use

Putting your data *'beyond use*' ensures that your data cannot be retrieved in a useable format or reconstituted, and is a method of deletion recognised by the ICO. This means that your data cannot be used in any manner that affects you, or informs any decision made in respect of you. Data that is put beyond use cannot be used for marketing or other commercial purposes. The data is placed in a secure, locked down state. No further processing activities (including accessing, viewing or sharing data) will be performed by us on the data unless in furtherance of a Court Order or other legal instrument.

To be clear, we will not give any other organisation access to your personal data and we surround the personal data with appropriate technical and organisational security

Proxy access data

If you wish to request deletion of data that either:

a) you, acting as a proxy for somebody else, have entered into that person's record within the App, or
b) somebody else, acting as a proxy for you, has entered into your record within the App

please email dpo@tpp-uk.com.

Research data

In order to share data with a research organisation from within the 'Help the NHS' section of the App, you first have to consent to the researcher's terms and conditions, which explain how that organisation will process the data you contribute through the App. You should be given the option to Opt-out of the research project at any stage. If you choose to do this you will no longer receive notifications from that organisation, nor be able to view any clinical content published by the organisation. Any future data you enter into the App will not be shared to that research organisation.

Disabling your App account will also end your consent to share further data with these research organisations.

How these organisations process your data will be outlined in each organisation’s consent form. If you have consented to the use of your personal information for research, any data already shared to that research organisation will not be able to be removed by us. You will need to contact these organisations individually to request deletion of data that they may hold.

Circumstances where we may be unable to complete the request for deletion

We may reject requests for deletion that require disproportionate technical measures (for example, the need to develop new systems or fundamentally change existing practices), that pose risks to the legitimate rights and interests of others, or that are unrealistic.

We will not be able to respond to your request in the following circumstances, as required by laws and regulations:

- Related to national security and defence security;
- Related to public safety, public health, major public interests;
- Related to crime investigation, prosecution, trial and enforcement of sentences, etc.;
- Where there is sufficient evidence to show subjective malice or abuse of rights;
- If the response to your request will cause you or other individuals, organisations of the legitimate rights and interests serious damage;
- Involving trade secrets.