SystmConnect Privacy Policy

SystmConnect Privacy Policy 1

1. Personal Information 2

Information you give us: 2

Information we collect from you: 2

Information we receive from other sources. 3

NHS login: 3

2. Uses of personal information 3

Information we receive from other sources. 3

3. Use of non-personal information 3

4. How your data is processed 4

Disclosure of your information 4

5. Our legal basis for processing data 4

6. Data Retention 4

7. Your Rights 5

8. Information Security 5

9. Contact 5

10. Changes to our privacy policy 6

11. SystmConnect Deletion Policy **** 6

Data Deletion 6

Deletion Principles 6

Beyond Use 7

Circumstances where we may be unable to complete the request for deletion: 7

The Phoenix Partnership (Leeds) Ltd ("TPP") are committed to protecting and respecting your privacy. TPP has developed SystmConnect to provide improved access to Healthcare Organisations.

In addition to SystmConnect TPP provides software products to healthcare organisations involved in your care. These healthcare organisations are responsible for how your information is used and are the Data Controller for the data they collect about you. The Data Controller determines what information is collected and how it is used.

To provide SystmConnect and the associated services, we must process information about you. 'Processing' for the purposes of this notice covers a very broad range of activities, including using, transferring, storing and even deleting data. Please read the following carefully to understand and how we will treat your personal data.

This privacy policy (together with the terms and conditions for using our website and End User Licence Agreement) sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us.

Please note that some of our other products or services, such as Airmid, Brigid and Airmid Cares, will have their own privacy policies that will apply in place of this policy. By using the website, our services and/or contacting us you are accepting and consenting to the practices described in this policy including the collection, use and transfer of the relevant data described below.

1. Personal Information

The following information is used by us in order to provide SystmConnect and associated services:

Information you give us:

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

- personal information that we ask for to submit online requests (such as your name, gender, date of birth, NHS number and phone number/email address);
- demographic, medical and lifestyle information that you add using SystmConnect;
- information in or about the content you provide (e.g. metadata), such as the date and time when information is added
- information you provide to us via the website, our services, a telephone call, email or any other messaging facility.

Information we collect from you:

We may collect information from your use of SystmConnect including:

- Device and Connection information, such as the type of device, operating system, platform, mobile network information and phone number; Connection information such as the name of your mobile operator or ISP, browser type and version, browser plug-in types and versions, 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 websites that use the service, such as information collected by us when you visit or use third-party apps and websites that use our services;
- Information about transactions made on using SystmConnect.

Information we receive from other sources.

We may receive information about you if you use any of the other services we provide including:

- medical and lifestyle information contained within your medical record. This information has been recorded by organisations who are/have been caring for you

NHS login:

Please note that if you use your NHS login details to access SystmConnect, the NHS login identity verification services are managed by NHS England. NHS England is the controller for any personal information you provided to NHS England 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 England (as the controller) when verifying your identity. Tap here to see NHS England'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 to you and your healthcare provider
- To personalise features and content, services or suggest additional functionality that you may find helpful. In order to create personalised services that are unique and relevant to you, we use:
    - Information on how you use and interact with the SystmConnect 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.
- To allow you to participate in any interactive features of our services, when you choose to do so.
- To help us keep SystmConnect 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 services, and promote safety and security.
- For internal operations, including troubleshooting, data analysis, testing, research, statistical purposes;

Information we receive from other sources.

We may combine this information with information you give to us and information we collect about you. We may use this information and the combined information for the purposes set out above (depending on the types of information we receive).

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason that is compatible with the original purpose. If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

3. Use of 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 services are being used. We use the information to develop, test and improve SystmConnect and associated 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 processed

The data that you enter using SystmConnect will be visible to the Healthcare Organisation offering this service to you. This data will be incorporated into your medical record (which may then be shared by them with other organisations directly involved in your care).

Disclosure of your information

We may disclose or share your personal data if we are under a duty to comply with any legal obligation, or in order to enforce or apply our terms of use and other agreements; or to protect the rights, property, or safety of TPP, our customers, or others. We remain responsible for those third parties and it is our responsibility to ensure that they use any of your personal data that we make available to them correctly and in accordance with our instructions and the law.

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.

We do not use or disclose your information to anyone except as described in this Privacy Policy.

5. Our legal basis for processing data

We act as data processor for the data that your care organisation asks you to enter into SystmConnect. For example, responses to health related questions.

In addition we act as Data Controller for the information we collect from you (see section 'Information we collect from you' above).

We collect, use and share data that we have in the ways described above:

- As necessary to comply with our legal obligations which may be expressed in written contractual agreements;
- To protect your interests, or those of others;
- As necessary in the public interest; and
- As necessary for our (or others') legitimate interests unless those interests are overridden by your interests or fundamental rights and freedoms that require protection of personal data. Legitimate interests may include;
    - providing an innovative, personalised, safe and profitable service to our users and partners;
    - carrying out and/or testing our services, processes and policies;
    - following guidance of government and regulatory bodies;
    - audit purposes to ensure (amongst other things) we are responding where necessary and providing an effective business model;
    - market research and statistics.

6. Data Retention

Any data, including images, that you successfully share to your patient record will be retained until it is no longer necessary for the provision of care or is deleted by the Data Controller (whichever comes first). All other data will be retained until it is no longer necessary for the provision of care or you request its deletion (whichever comes first). This will be in line with the latest Records Management Code of Practice produced by NHS England as implemented by your healthcare provider.

Personal information that has been deleted may persist in our backup systems, but will not be readily accessible. Our services also use encrypted backup storage as another layer of protection to help recover from potential disasters. Data can remain on these systems for up to 6 months. When TPP delete data, we follow a deletion policy to make sure that your data is safely and completely removed from our servers.

7. Your Rights

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

How can you exercise your rights provided under the GDPR?

Under the General Data Protection Regulation, you have the right to access, rectify, port and delete your data.

You also have the right to object to and restrict certain processing of your data. This includes:

- the right to object to our processing of your data for direct marketing;
- the right to object to our processing of your data where we are performing a task in the public interest or pursuing our legitimate interests or those of a third party.
- the right to have your data amended if it is inaccurate. You can find more information about your rights on the Information Commissioner's Office website – please see https://ico.org.uk/for-the-public/

Please be aware that information recorded by you and added to the healthcare record of another party (your healthcare provider) remains their responsibility (as they are the data controller) and so you will need to direct any request regarding your rights under GDPR to them.

8. Information Security

We make it a priority to provide strong security and give you confidence that your information is safe. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this privacy policy. We use strict procedures and security features in accordance with best industry practice and standards. We store all of your information on secure servers and our security measures are to the standards set by the UK National Cyber Security Centre.

All TPP employees, contractors, and agents are subject to strict contractual confidentiality obligations and may be disciplined or prosecuted or their employment terminated if they fail to meet these obligations. We restrict access to your personal information to only those who need that information in order to process it.

Unfortunately, if you are accessing the website from a mobile device, the transmission of information via your device is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to us; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

9. Contact

If you have any concerns please contact our Data Protection Officer (DPO) and data protection team:

By post – TPP House, 129 Low Lane, Horsforth, Leeds, LS18 5PX

By email – dpo@tpp-uk.com

TPP is registered with the Information Commissioner's Office (ICO), which regulates data protection in the UK, and our registration number is Z1927388.

You can raise a complaint with the Regulator here: https://ico.org.uk/make-a-complaint/

We will investigate and attempt to resolve any data privacy objections and complaints relation your details provided in accordance with the above and make reasonable effort to allow you to exercise your rights as quickly as possible and within the timescales provided by data protection laws.

10. Changes to our privacy policy

Our privacy policy may change from time to time. We will post any privacy policy changes on the website. Please check the website frequently to see any updates or changes to our privacy policy.

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

11. SystmConnect 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.

This Deletion Policy explains how data can be removed or deleted. 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 Deletion

We recognise there are certain circumstances where you may request that we delete the data we hold about you as Data Controller 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 we permanently no longer provide you with products or services.

Deletion Principles

- By requesting data that you have entered to be deleted, you understand this will mean that the data will no longer be accessible,
- The data in scope for deletion by us is personal data entered by you and associated metadata as defined in 'Information we collect from you' above.
- The data outside the scope for deletion is;
    - Data you have added in response to a request from a health or care provider
    - Data shared to your healthcare organisation and entered into your medial record;
- Any in-scope data will be deleted by it being put beyond use.
- Any requests for deletion of out-of-scope data will need to be raised with e the health or care provider who holds your medical record.
- Following deletion, we will no longer be able to assist you with access to such data and all processing activities by us shall cease.
- 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.

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