



# Privacy Policy

## Introduction

Welcome to the Pathway Software (UK) Limited's (the Company) privacy policy.

The Company is committed to protecting and respecting the privacy of all our customers, partners and the end users of our Services and Software.

This privacy policy will inform you as to how we look after your Personal Data and tells you about your privacy rights and how the law protects you.

## Important information and who we are

### Purpose of this privacy policy

This policy together with:

- our Terms of Service applicable to your use of the Services where you are our Customer (our **Terms of Service**); and
- our Acceptable Use Policy applicable to your use of the Software (our **Acceptable Use Policy**)

- and any other documents referred to in the Terms of Service and/or the Acceptable Use Policy sets out the basis on which any Personal Data the Company collects from you, or that you provide to the Company, whether through this Site or when you use our Services and/or Software will be processed by us.

The Site is not intended for children and we do not knowingly collect data relating to children.

It is important that you read this privacy policy together with any other privacy policy or fair processing policy we may provide on specific occasions when we are collecting or processing Personal Data about you so that you are fully aware of how and why we are using your data. This privacy policy supplements other notices and privacy policies and is not intended to override them.

### Changes to the privacy policy and your duty to inform us of changes

We keep our privacy policy under regular review. We may change this policy from time to time to take account of:

- changes to Data Protection Legislation and other laws which may affect this policy;
- guidance issued by the ICO and others;
- issues raised by our Customers, partners and end users



Accordingly we suggest that you regularly check this page to ensure that you continue to be comfortable with the measures that we are taking to protect your privacy. This policy was last updated on 29 January 2021.

It is important that the Personal Data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

## Definitions

In this policy the following words have the following meanings:

**Customer** includes the following (a) customers who have entered into a contract with us for the supply of the Services and WriteUpp (b) customers who have subscribed for a trial of our Services and WriteUpp, in both cases in accordance with our Terms of Service.

**Controller, Processor, Data Subject, Personal Data, Personal Data Breach, processing and appropriate technical and organisational measures:** as defined in the Data Protection Legislation.

**Data Protection Legislation:** the UK Data Protection Legislation and any other European Union legislation relating to Personal Data and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications)..

**UK Data Protection Legislation:** all applicable data protection and privacy legislation in force from time to time in the UK including the General Data Protection Regulation ((EU) 2016/679) (UK GDPR); the Data Protection Act 2018; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended.

**Patients** means the Customer's patients.

**Patients Data** means Personal Data of Patients, including clinical notes and assessments.

**Personal Data** means any information relating to an identified natural person that is processed by the Company as a result of, or in connection with the provision of the Services; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**ICO** means the Information Commissioner's Office and any successor to it as data protection authority.

**Us, Our, We or Company** means Pathway Software (UK) Limited and our Staff.

**You, Your, or Customer** means your organisation and its Staff.

**Software, Services or WriteUpp** means the software and associated services provided and developed by the Company which may be supplied to you.

**Standard Contractual Clauses (SCC)** the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors



established in third countries (controller-to-processor transfers) as set out in the Annex to Commission Decision 2010/87/EU.

**Staff** means your and our employees, workers, agents and sub-contractors.

**Site** means the Company's website at <https://www.writeupp.com>.

### **The Company – as Data Controller**

Where you are a Customer of the Company, we will be the Data Controller in respect of certain Personal Data which you and your Staff may supply to us or which we collect from you which relates to you and your Staff (**Customer Data**).

Pathway Software (UK) Limited of Watergate House, 85 Watergate Street, England, CH1 2LF (registered in England and Wales with company number 06844098) is the Controller in respect of Customer Data.

As Data Controller, we determine the purposes for which and the manner in which Customer Data is, or is to be, processed. In this policy we describe the types of processing we may undertake with respect to Customer Data.

### **The Customer– as Data Controller, the Company as Data Processor**

Where you or your Staff are responsible for the input of Patient Data which may be collected, stored and processed as a result of your use of the Services and WriteUpp, you will be the Data Controller. The Company will be a Data Processor only.

In cases where you are collecting, storing and processing Patient Data you will determine the purposes for which and the manner in which that Personal Data is, or is to be processed. You will also be responsible for:

- informing your Staff and Patients of your own privacy policy and practices, including the lawful grounds upon which you are processing any Personal Data;
- compliance with Data Protection Legislation including all data protection and privacy laws relevant to the territory in which you operate and/or which are applicable to your Patients;
- drawing the Patient's attention to this privacy policy;
- informing us if any Patient objects to either your or our processing.

Patient Data is to be distinguished from Customer Data which the Company has collected from you (our Customer). For example, you may have agreed to our collection, use, transfer and storage of Customer Data (including data of your Staff) for the Company's own business purposes including credit checks, administration of contractual arrangements, sales and marketing.

### **Conditions for Processing**

The Customer will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Patient Data to the Company and/or lawful collection of the Patient Data by the Company on behalf of the Customer for the duration and purposes of the Services. The Customer acknowledges that for the purposes of the Data Protection Legislation, the Customer is the Controller and that the Company is the Data Processor. The Company shall, in relation to any Patient Data processed in connection with the performance by the Company of the Services:



- process that Patient Data only on your written instructions;
- ensure that it has in place appropriate technical and organisational measures, to protect against unauthorised or unlawful processing of Patient Data and against accidental loss or destruction of, or damage to, Patient Data, as are appropriate;
- ensure that all the Company's Staff who have access to and/or process Patient Data are obliged to keep the Patient Data confidential;
- not transfer or otherwise process Patient Data outside of the European Economic Area (EEA) without obtaining the Customer's prior written consent. Where such consent is granted, the Company may only process, or permit the processing, of Patient Data outside the EEA under the following conditions:
  - the Company is processing Patient Data in a territory which is subject to a current finding by the European Commission under the Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals; or
  - the Company participates in a valid cross-border transfer mechanism under the Data Protection Legislation, so that the Company (and, where appropriate, the Customer) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the General data Protection Regulation ((EU) 2016/679); or
  - the transfer otherwise complies with the Data Protection Legislation (collectively "Appropriate Safeguards")
- assist the Customer, at the Customer's cost, in responding to any request from a Data Subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;
- notify the Customer without undue delay on becoming aware of a Personal Data Breach;
- within 45 days of the date of termination or cancellation of your Contract delete Patient's Data and copies thereof unless required by Data Protection Legislation to store the Personal Data; and
- maintain complete and accurate records and information to demonstrate its compliance with these obligations.

The Customer authorises the Company to transfer the Patient Data outside the EEA provided all transfers by the Company of the Patient Data shall be (to the extent required under Data Protection Legislation) effected by way of Appropriate Safeguards.

The Company (and any sub-processors) may only transfer the Patient Data to (or process Patient Data) in the following countries: United Kingdom, United States of America, Republic of Ireland and the Netherlands

If any Patient Data transfer between the Customer and the Company requires execution of Standard Contractual Clauses in order to comply with Data Protection Legislation (where the Customer is the entity exporting Patient Data to the Company outside the EEA), the following shall apply in order to provide an appropriate safeguard:

- the parties shall enter the Standard Contractual Clauses agreement;
- the agreement referred to above will be effective upon it being signed by both parties; and
- a copy of the executed agreement shall be delivered to each of the parties.



You acknowledge that the Company uses various third-party suppliers to provide functionality within WriteUpp for the Customer's optional use to deliver and send text and email messages. The Customer accepts that such use will be in accordance with the third-party suppliers' terms and conditions and their respective privacy policies. The Customer will ensure that it has Patients consent or other authority to share Patients Data via these communications.

Where the Company engages another Data Processor for carrying out processing activities on behalf of the Customer, the same data protection obligations as set out in this Contract shall be imposed on that other Data Processor by way of a contract or other binding legal means, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of Data Protection Legislation. Before the commencement of any sub-processing the Company shall make sufficient enquiries to ensure that the sub processor is capable of carrying out its data processing obligations.

At any time on not less than 30 days' notice, the Company may revise this part of the privacy policy by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when this policy is updated).

The Company is not liable in respect of any Patient Data which is controlled by the Customer in breach of Data Protection Legislation or outside the scope of the permissions granted to you by the Patient.

## The Kind of Information we hold

We may process the following types of Personal Data:

### 1. Customer Data:

This is information you give us about you and your Staff and may include:

- **Identity Data** including name, username;
- **Contact Data** including address, email address and telephone number
- **Transaction Data** includes details about payments to and from you and other details of products and services you have purchased from us.
- **Technical Data** includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access this website.
- **Profile Data** includes your username and password, purchases or orders made by you, your interests, preferences, feedback and survey responses.
- **Usage Data** includes information about how you use our website, products and services.
- **Marketing and Communications Data** includes your preferences in receiving marketing from us and our third parties and your communication preferences.

We use different methods to collect data from and about you including through:



**Direct interactions.** You may give us your Identity and Contact by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes Personal Data you provide when you:

- Visit our Site;
- Use our Services;
- Use WriteUpp;
- Correspond with us by filling in forms, post, phone, e-mail or otherwise;
- Request marketing to be sent to you;
- Participate in any discussion boards or other social media functions on our Site;
- submit an enquiry to us regarding our products and/or Services whether by telephone, email, via our website or other channel;
- register a profile, complete surveys, or tell us about any problems with our Site;
- submit material for publication on our website (whether in discussion boards, chat rooms or other social media platforms our website);
- subscribe for any newsletter or publication we may supply.

**Automated technologies or interactions.** As you interact with our website, we will automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this Personal Data by using cookies, server logs and other similar technologies. We may also receive Technical Data about you if you visit other websites employing our cookies. Please see our cookie policy for further details.

**Third parties or publicly available sources.** We will receive Personal Data about you from various third parties as set out below:

**Usage Data.** Personal Data is collected by Raygun – error and performance monitoring for WriteUpp.

## **2. Patient Data:**

This is information you enter into WriteUpp about your Patients when using WriteUpp and our Services which may include, but is not limited to:

- Name
- Address
- Email address
- Landline & Mobile Number
- Insurer details
- GP details
- Medical records
- Treatment plans
- Letters & documentation
- Communications with other healthcare professionals; and
- Other information necessary for the operation of the Services and/or WriteUpp.

This Patient Data may be supplied by you when you:



- Use our Services in the course of your business;
- Use WriteUpp in the course of your business; or
- when you report a problem with our Site.

This Patient Data may be processed by us for the purposes of:

- storing Patient Data on WriteUpp;
- storing Patient Data on our servers;
- supplying you with our products and Services;
- enabling and assisting us to comply with all legal, regulatory and compliance obligations to which we are subject; and
- ensuring the security of our Services, maintaining back-ups of our databases and sending communications to you.

## How we will use personal data

### Lawful Basis for the Company's processing activities.

In this privacy policy, the following terms have the following meanings:

**Legitimate Interest** means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your Personal Data for our legitimate interests. We do not use your Personal Data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.

**Performance of Contract** means processing your Personal Data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

**Comply with a legal obligation** means processing your Personal Data where it is necessary for compliance with a legal obligation that we are subject to.

When the Company processes Personal Data, whether as Data Controller or as Data Processor, we will rely on the following lawful grounds for processing of each of the categories of data identified above.

### The Company will use personal information in the following ways:

#### 1. Customer Data

We have set out below, in a table format, a description of all the ways we plan to use Customer Data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your Personal Data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.





Generally, we do not rely on consent as a legal basis for processing your Personal Data although we will get your consent before sending third party direct marketing communications to you via email or text message. You have the right to withdraw consent to marketing at any time by following the opt-out links on any marketing message sent to you..

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To register you as a new customer	(a) Identity (b) Contact	Performance of a contract with you
To process and deliver your order including: (a) Manage payments, fees and charges (b) Collect and recover money owed to us	(a) Identity (b) Contact (c) Transaction (d) Marketing and Communications	(a) Performance of a contract with you  (b) Necessary for our legitimate interests (to recover debts due to us)
To manage our relationship with you which will include: (a) Notifying you about changes to our terms or privacy policy (b) Asking you to leave a review or take a survey	(a) Identity (b) Contact (c) Profile (d) Marketing and Communications	(a) Performance of a contract with you  (b) Necessary to comply with a legal obligation  (c) Necessary for our legitimate interests (to keep our records updated and to study how customers use our products/ services)
To enable you to partake in a prize draw, competition or complete a survey	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications	(a) Performance of a contract with you  (b) Necessary for our legitimate interests (to study how customers use our products/services, to develop them and grow our business)
To administer and protect our business and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity (b) Contact (c) Technical	(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise)  (b) Necessary to comply with a legal obligation





To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications (f) Technical	Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy)
To use data analytics to improve our website, products/services, marketing, customer relationships and experiences	(a) Technical (b) Usage	Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy)
To make suggestions and recommendations to you about goods or services that may be of interest to you	(a) Identity (b) Contact (c) Technical (d) Usage (e) Profile (f) Marketing and Communications	Necessary for our legitimate interests (to develop our products/services and grow our business)

## 2. Patient Data:

The legal basis for this processing is:

- you have obtained all necessary and appropriate consent from the Patient/data subject in accordance with Data Protection Legislation;
- because this is necessary for your use of WriteUpp and the supply of our Services to you, and performance of our contract; and/or
- your legitimate interests, namely the supply of your services to your Patients.

Patient Data may be processed by the Company for the purposes of:

- storing Patient Data on WriteUpp;
- storing Patient Data on our servers;
- supplying you with our products and Services;
- enabling and assisting us to comply with all legal, regulatory and compliance obligations to which we are subject; and
- ensuring the security of our Services, maintaining back-ups of our databases.

### If you fail to provide personal information



If you, the Customer, fail to provide certain information when requested, the Company may not be able to perform the Services and any contract we have entered into with you or we may be prevented from complying with our legal obligations.

### **Change of purpose**

Where we are Data Controller (in respect of Customer Data only): the Company will only use personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Where we are Data Processor: the Company will only process Patient Data in accordance with the conditions for processing set out in this policy. We shall only process Patient Data relevant to a particular Customer's Patients, while our contract with the Customer is continuing and shall cease such processing (a) when requested by the Customer (b) on termination of the contract (c) on cancellation of the contract; or (d) at the request of the data subject.

### **Marketing**

We strive to provide you with choices regarding certain Personal Data uses, particularly around marketing and advertising.

### **Promotional offers from us**

We may use your Identity, Contact, Technical, Usage and Profile Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you (we call this marketing).

You will receive marketing communications from us if you have requested information from us or purchased services from us and you have not opted out of receiving that marketing.

### **Third-party marketing**

We will get your express opt-in consent before we share your Personal Data with any third party for marketing purposes.

### **Opting out**

You can ask us or third parties to stop sending you marketing messages at any time by following the opt-out links on any marketing message sent to you.

Where you opt out of receiving these marketing messages, this will not apply to personal data provided to us as a result of service purchase, service experience or other transactions.

## **Disclosure of your personal data**

You agree that the Company has the right to share Customer Data (but not Patient Data) with:



- Any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.
- Selected external third parties including:
  - business partners, suppliers and sub-contractors for the performance of any contract we enter into with them or you (including third party IT providers, hosting and back-up service providers);
  - Professional advisers including lawyers, bankers, auditors and insurers who provide consultancy, banking, legal, insurance and accounting services; and
  - third party service providers who assist us with our activities, such as hosting providers, and other IT or payment service providers, may also have access to Personal Data held by us and may use this information on our behalf
- Third parties to whom we may choose to sell, transfer or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this privacy policy.
- Other third parties:
  - if we are under a duty to disclose or share your personal data in order to comply with any legal obligation, or in order to enforce or apply the Terms of Service or the Acceptable Use Policy and other agreements; or
  - to protect the rights, property, or safety of the Company, our customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction;
  - to assist us in improving our products and Services. We monitor aggregated data that is collected by our Service and may share this with third parties collectively and in an anonymous way. This data will not reveal personal information.

We will not sell, rent or share Customer Data or Patient Data with third parties in other ways without your consent unless we are entitled by law to do so.

We require all third parties to respect the security of your Personal Data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

## **Where the Company will store personal data**

We may hold Personal Data in electronic databases, such as our customer relationship management system. We take all reasonable steps to keep any Personal Data we hold about you (and your Patients) secure.

All information which is provided to, or collected by, the Company is:

- Stored on the Company's secure servers within the United Kingdom and the European Union (EU), namely Dublin and Amsterdam.
- Hosted on secure data centre managed by our hosting partner with 24/7 manned security, CCTV, biometric access to the facility and restrictive access to the internals of the building based on authorisation levels.



## **International transfers**

European Union (“EU”) data protection rules apply to the European Economic Area (“EEA”), which includes all EU countries and the non-EU countries of Iceland, Liechtenstein and Norway.

The UK and the EU agreed a Trade and Cooperation Agreement effective from the 1st January 2021. This agreement provides for an interim period of up to six months where Personal Data can be transferred from the EEA to the UK and not be seen as a transfer to a third country. Essentially, the same position on transfers that applied during the Brexit transition period which is being preserved on an interim basis whilst a UK adequacy decision is considered.

In relation to UK to EEA transfers, the UK has already announced that it will initially treat the EEA countries as adequate for the purpose of UK to EEA transfers, but that this will be kept under review.

Many of our external third parties are based outside the UK so their processing of your Personal Data will involve a transfer of data outside the UK.

Whenever we transfer your Personal Data out of the UK, we ensure a similar degree of protection is afforded to it by ensuring safeguards are implemented.

We will only transfer your Personal Data to countries that have been deemed to provide an adequate level of protection for Personal Data.

Please contact us if you want further information on the specific mechanism used by us when transferring your Personal Data out of the UK.

## **Data Security**

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

### **Passwords and Security**

Where the Company has given you (or where you have chosen) a password which enables you to access your account, you are responsible for keeping this password confidential. The Company asks you not to share a password with anyone.

Unfortunately, the transmission of information via the internet is not completely secure. Although the Company will do its best to protect your Personal Data, the Company cannot guarantee the security of your data transmitted via the Site; any transmission is at your own



risk. Once the Company has received your information, the Company will use strict procedures and security features to try to prevent unauthorised access.

## Data Retention

### How long the Company will use personal data

The Company will retain Customer Data for:

- such time as this is required in connection with the Services we are supplying to you;
- following completion of the Services for a period of not less than 6 years from the date the Services end.

We may retain Customer Data where such retention is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.

The Company will retain Patient Data for:

- such time as this is required in connection with the Services we are supplying to you;
- following completion of the Services for a maximum period of 45 days from the date the Services end.

## Your rights as a data subject (where the Company is the Data Controller)

Under certain circumstances, if you are an individual in respect of whom the Company processes Personal Data, you have the following rights. Please note that this is a summary of your rights. If you wish to understand your rights in detail you should read the relevant laws, guidance and regulations for a fuller explanation.

You have the right to:

**Request access** to your Personal Data (commonly known as a "data subject access request"). This enables you to receive a copy of the Personal Data we hold about you and to check that we are lawfully processing it. We will supply the data free of charge but we reserve the right to charge a reasonable fee (or refuse to act on the request) if you request additional copies of the information, if access requests are unfounded or excessive.

There are circumstances where we may withhold the supply of your Personal Data – for instance where the rights and freedoms of others may be affected or where we are permitted by law.

**Request correction** of the Personal Data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

**Erasure** of your Personal Data. This enables you to ask us to delete or remove Personal Data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your Personal Data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your Personal Data to comply with local law.



Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

**Object to processing** of your Personal Data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

**Request restriction of processing** of your Personal Data. This enables you to ask us to suspend the processing of your Personal Data in the following scenarios:

- If you want us to establish the data's accuracy.
- Where our use of the data is unlawful but you do not want us to erase it.
- Where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims.
- You have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

**Request the transfer** of your Personal Data to you or to a third party. We will provide to you, or a third party you have chosen, your Personal Data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

**Withdraw consent at any time** where we are relying on consent to process your Personal Data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.



### **No fee usually required**

You will not have to pay a fee to access your Personal Data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

### **What we may need from you**

We may need to request specific information from you to help us confirm your identity and ensure your right to access your Personal Data (or to exercise any of your other rights). This is a security measure to ensure that Personal Data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

### **Time limit to respond**

We try to respond to all legitimate requests within one month. Occasionally it could take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

### **Withdrawal of consent**

In any cases where the legal basis for our processing of your Personal Data is consent, you have the right to withdraw that consent at any time. Such withdrawal will not affect the lawfulness of any processing before you withdraw consent.

## **Cookies**

Like most applications, WriteUpp uses cookies to help provide you with the best experience we can. Cookies are small text files that are placed on your computer or mobile phone when you browse websites

Our cookies help us:

- Make WriteUpp work as you'd expect
- Enables WriteUpp to remember your details so you don't have to enter them each time you log in (if you so choose)
- Remember your settings in WriteUpp
- Improve the speed/security of WriteUpp

We do not use cookies to:

- Collect any personally identifiable information (without your express permission)
- Pass data to advertising networks
- Pass personally identifiable data to third parties

You can learn more about all the cookies we use below.





## **Granting us permission to use cookies**

If the settings on your software that you are using to view this Site (your browser) are adjusted to accept cookies we take this, and your continued use of our Site, to mean that you are fine with this. Should you wish to remove or not use cookies from our Site you can learn how to do this below, however doing so will prevent the service from working.

## **Website Function Cookies**

### **Our own cookies**

We use cookies to make our Site work, including:

- Determining if you are logged in or not
- Remembering your search settings
- Showing which patients you have recently viewed
- Tailoring content to your needs
- Remembering your preferences

There is no way to prevent these cookies being set other than to not use our Site.

### **Third party functions**

Our Site, like most websites, includes functionality provided by third parties. Disabling these cookies will likely break the functions offered by these third parties.

### **Turning cookies off**

WriteUpp will not function if cookies are turned off or disabled.

## **Links**

The Site may, from time to time, contain links to and from the websites of our partner networks, advertisers and affiliates. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. Please note that we do not control these third-party websites, which may have their own privacy policies, and that we are not responsible for their privacy statements. When you leave our Site, we encourage you to read the policy statement of every website you visit.

## **Contact**

Questions, comments and requests regarding this privacy policy are welcomed and should be addressed to [support@writeupp.com](mailto:support@writeupp.com).

If you have any questions or have a complaint about this privacy policy please let us know us immediately.

To individuals situated in the EU, please contact us directly in regards to requesting your individual rights, alternatively we have instructed Verasafe Ireland Limited as our EU



Representative in accordance with Article 27 of the GDPR for EU supervisory authorities and EU citizens (contact details below).

Post: Verasafe Ireland Limited, Unit 3D North Point House, North Point House, North Point Business Park, New Mallow Road, Cork, T23 ATZP.

You have the right to make a complaint at any time to the Information Commissioner's Office (**ICO**), the UK supervisory authority for data protection issues ([www.ico.org.uk](http://www.ico.org.uk)). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

### **Company Information**

Pathway Software  
Watergate House,  
85 Watergate Street,  
England,  
CH1 2LF

Web: [www.writeupp.com](http://www.writeupp.com)  
Email: [support@writeupp.com](mailto:support@writeupp.com)  
Company Number: 06844098  
VAT Number: 948 3831 85