Privacy Notice (Patients)

Organisation: Augmentia
Issue Date: Sep 1, 2025
Document Owner: Alex Radcliffe

Document Version Control

Version	Date	Description	Author	Approver
1.0.0	Sep 1, 2025	First Version	Alex Radcliffe	Steve Marsh

Privacy Notice

This Privacy Notice describes the organisation's policies and procedures on the collection, use and disclosure of patient data received with Data Share Agreements, and informs users and public about privacy rights and how the law protects individual rights and freedoms.

Contents

Privacy Notice

This Privacy Notice describes Augmentia's policies and procedures on the collection, use and disclosure of patient data received through Data Sharing Agreements. It explains patients' privacy rights and how the law protects those rights. This Privacy Notice gives you information about how Augmentia collects and uses patient data through the use of our app, and acts as a data processor on behalf of GP practices and other healthcare providers (the data controllers).

Who we are and how to contact us

Augmentia is the processor of the patients' personal data (collectively referred to as, "we", "us" or "our" in this Privacy Notice). Augmentiais a company registered in England and Wales with company number 15010967with its registered office at 20 Wenlock Road London N1 7GU.
If you would like to contact us about anything in this Privacy Notice, or if you have any questions about our role as a processor, you may contact our Data Protection Officer at: dpo@augmentia.ai

The types of personal data we collect about the patients

Personal data means any information about an individual from which that person can be identified.
We may collect, use, store and transfer different kinds of personal data about patients which we have grouped together as follows:

- **Identity Data** includes Email address, first name, last name, username or similar identifier, marital status, title, date of birth and gender.
- **Contact Data** includes home address, email address, and telephone numbers.
- **Health Data** includes any data about patient's health that is shared with us for the use of our services.

We also collect, use and share **anonymised aggregated data** such as statistical or demographic data which is not personal data as it does not directly (or indirectly) reveal your identity. For example, we may use this anonymised data for the purposes of helping us build evidence to justify formal clinical trials and feasibility studies in a clinical setting, or for internal research and product development, including product development involving machine learning and big data analysis, or for future publications.

1.0 How is patients' personal data collected?

Patient data is received from GP practices via NHS systems such as the IM1 API, under data sharing agreements.

1.1 Responsibilities Matrix: Controller vs Processor

The following table summarises the key responsibilities under data protection law and identifies whether Augmentia(Processor) or the GP Practice/Healthcare Provider (Controller) holds responsibility.

Responsibility	Controller (GP Practice)	Processor (Augmentia)
Determine purpose and legal basis of processing	✔	
Obtain valid patient consent if applicable	✔	
Respond to subject access or other data rights requests	✔	
Maintain contact with the Information Commissioner's Office (ICO)	✔	
Process personal data only on documented instructions		✔
Implement technical and organisational security measures		✔
Assist controller with subject rights and data breaches		✔
Maintain records of processing activities (Article 30 GDPR)	✔	✔
Engage sub-processors and ensure proper contracts		✔
Notify controller of any data breach without undue delay		✔

2.0 How we use your personal data

2.1 Legal basis

The law requires us to have a legal basis for collecting and using the personal data. We rely on one or more of the following legal bases:

- **Performance of a contract:** Where we need to perform the contract we are about to enter into or have entered into with GP practices and other health services bodies.
- **Legitimate interests:** We may use patient personal data where it is necessary to conduct our business and pursue our legitimate interests, for example to prevent fraud and enable us to give the best and most secure customer experience. We make sure we consider and balance any potential impact on patients and patient rights (both positive and negative) before we process the personal data for our legitimate interests. We do not use personal data for activities where our interests are overridden by the impact on patient (unless we have the consent, right or are otherwise required or permitted to by law).
- **Legal obligation:** We may use the personal data where it is necessary for compliance with a legal obligation that we are subject to. We will identify the relevant legal obligation when we rely on this legal basis.
- **Consent:** We rely on consent only where we have obtained active agreement to use personal data for a specified purpose.

2.2 Purposes for which we will use your personal data

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

Purpose/Use	Type of data	Legal basis
To process and deliver our services: (a) Provide users with most accurate and up-to-date information about patient (b) Enable users to track the current surveillance status of patients as required by NHS frameworks, and take action.	(a) Identity (b) Contact (b) Health	Data Processing agreement with GP Practices enabled based on Article 6 (1) (e) and Article 9 (2) (h) of the GDPR.
To administer and protect our business and this product (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity (b) Contact (b) Health	(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

2.2.1 Augmentia as a data processor:

Augmentia acts as a data processor when processing patient data which means we only process patient data according to the instructions of the data controller – the organisations providing care, such as GP practices or PCNs and Health Trusts. They maintain the overall responsibility for patient data and the circumstances of any processing. As such, Augmentia trictly under the instructions of the data controller. The controller determines the lawful basis for processing.
In most cases the organisation relies on:

- Article 6 (1) (e) of the GDPR, – processing personal information that is necessary to provide a service which is in the public interest
- Article 9 (2) (h) of the GDPR – permits processing of health information which is necessary for the provision of health treatment.

The national data opt-out is a service that allows patients to opt out of their confidential patient information being used for research and planning. As a processor it is not Augmentia's responsibility to process the opt out as that is the job of the data controller. However, you can find out more about opting out here.

3.0 Disclosures of your personal data

We may share patients' personal data where necessary with external third parties who provide services to us, e.g: cloud service providers and technology services, or clinical research organisations. We require all third parties to respect the security of the data and to treat it in accordance with the law. We have Data Processing Agreements in place with these third party providers and we do not allow our third-party service providers to use the personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions. We do not sell your data to anyone and only share it with our contracted processors.
Augmentia processes personal data in the capacity of a data processor. When we are a processor of personal data, we are doing so purely on the instructions of another organisation or company as they are the controller.
We also may share the personal data where necessary with the parties set out below for the purposes set out in the table above.

3.1 Business Transactions

If the Company is involved in a merger, acquisition or asset sale, your Personal Data may be transferred. Alternatively, we may seek to acquire other businesses or merge with them. We will provide notice to the related authorities before the Personal Data is transferred and becomes subject to a different Privacy Policy.

3.2 Law enforcement

Under certain circumstances, the Company may be required to disclose Your Personal Data if required to do so by law or in response to valid requests by public authorities (e.g. a court or a government agency).

3.3 Other legal requirements

The Company may disclose Personal Data in the good faith belief that such action is necessary to:

- Comply with a legal obligation
- Protect and defend the rights or property of the Company
- Prevent or investigate possible wrongdoing in connection with the Service
- Protect the personal safety of Users of the Service or the public
- Protect against legal liability

4.0 International transfers

We may transfer the personal data to service providers that carry out certain functions on our behalf. This may involve transferring personal data outside the UK or EEA to countries which have laws that do not provide the same level of data protection as the UK or EU law.
Although it is not transferred outside the UK currently, if we do in future, whenever we transfer your personal data out of the UK or EEA to service providers, we ensure a similar degree of protection will be afforded to it by ensuring that the following safeguards are in place:

- We will only transfer your personal data to countries that have been deemed by the UK or the EU to provide an adequate level of protection for personal data; or
- We may use specific standard contractual terms approved for use in the UK and/or EEA which give the transferred personal data the same protection as it has in the UK or EEA, or another transfer mechanism which has been approved by the relevant regulator in the UK and/or the EEA. To obtain a copy of these contractual safeguards, please contact us at dpo@augmentia.ai.

5.0 Data security

We have put in place appropriate security measures to prevent the personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to the 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.

6.0 Data retention

6.1 How long will the personal data be used for?

Patients' information is securely stored. Augmentiawill retain the Personal Data only for as long as is necessary for the purposes set out in this Privacy Notice.
We will retain and use the Personal Data to the extent necessary to comply with our legal obligations (for example, if we are required to retain the data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies. The Company will also retain Usage Data for internal analysis purposes. Usage Data is generally retained for a shorter period of time, except when this data is used to strengthen the security or to improve the functionality of Our Service, or We are legally obligated to retain this data for longer time periods.
To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of the personal data, the purposes for which we process the personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.
In some circumstances we will anonymise the personal data (so that it can no longer be associated with the patient) for research or statistical purposes, in which case we may use this information indefinitely without further notice.

7.0 Protecting the sensitive data

Augmentia follows the information security values of

- confidentiality - making sure the information is always kept secret and private;
- integrity - we ensure the completeness, consistency, and accuracy of the data over its lifecycle; and
- availability - we ensure the right information is available to the right person at the right time.

We use the following techniques and best practices to protect your sensitive data:

7.1 People

To assure the data protection, we take the precautions as listed:

- Training - All staff receive regular appropriate training on data protection and security and their related duties to ensuring the personal data is secure;
- Minimised access: the personal data, including Health Data, can only be accessed on a strictly needs to know basis by our admin staff, or customer support as and when necessary, specifically as relates to the particular request for support;
- Security expertise: To design and operate our platform, we utilise qualified security professionals with recognised experience and certifications in technical security architecture as well as governance, risk, and compliance.

7.2 Cyber resiliency, business continuity, and disaster recovery

- Our web frontend(s) and parts of our backend are hosted on Cloudflare and make use of their secure platform.
- Other Cloud Services or our private servers which may be in use from time to time are automatically kept up-to-date with the latest security patches and fixes.
- In addition, we commit to undertaking annual third-party security audits with certified security auditors including web, desktop and mobile application penetration tests to ensure comprehensive coverage.

7.3 Technology

We adopt principles of Secure by Design, including:

- Architecture in line with industry standards.
- This includes role based access controls.
- Our REST APIs utilise authentication and authorization to ensure data minimization and prevent unauthorised access to data.
- Our password quality validation for users ensures only strong passwords are allowed and are stored hashed using SHA-256.

We use encryption in all of the following scenarios:

- In transit using modern protocols (TLS only) and secure ciphers (both internally within the VPC and externally with users & applications)
- At rest using AES-256 encryption

Data centres:

- We host data in multiple availability zones/regions in order to maximise availability. All production environments are located within the UK and EEA.
- Where possible, deploy a High Availability (HA) architecture to ensure resilience with automated failover to provide uninterrupted service.

Development, security & operations:

- We operate a mature secure software development life cycle (SDLC), which includes but is not limited to:
  - Separation of keys for each environment and robust key management processes
  - Regular dependency and package management audits and remediation
  - Logical separation of production and development environments including isolated databases
  - Static code testing to ensure code is free from known vulnerabilities
  - Dynamic code testing to ensure applications do not expose vulnerabilities
  - Manual security testing (annual penetration test)

8.0 Your legal rights

Under data protection laws, you have a number of rights in relation to your personal data. These include the right to:

- **Request access** to your personal data (commonly known as a "subject access request"), allowing you to receive a copy of the personal data held about you and to check that it is being lawfully processed.
- **Request correction** of any incomplete or inaccurate personal data.
- **Request erasure** of your personal data in certain circumstances, such as where there is no valid reason for continued processing or where your data was unlawfully processed.
- **Object to processing** of your personal data where processing is based on legitimate interests, including profiling.
- **Object at any time to direct marketing** using your personal data.
- **Request the transfer** of your personal data to another party, in a structured, commonly used, machine-readable format (where applicable).
- **Withdraw consent** at any time where processing is based on your consent. This does not affect the lawfulness of any processing carried out before withdrawal.
- **Request restriction of processing** of your personal data, for example where you contest its accuracy or where processing is unlawful but you do not want it erased.

Important: As Augmentia acts solely as a **data processor** on behalf of GP practices and other authorized healthcare service providers (the **data controllers**), we do not determine how your personal data is used. We process your data only on the instructions of the controller.
To exercise any of the rights listed above, you should contact your GP practice or other healthcare provider directly, as they are responsible for handling such requests under data protection law.
If you have questions about how your data is processed by us on behalf of the controller, you may contact our Data Protection Officer at: dpo@augmentia.ai

8.1 No fee usually required

You will not have to pay a fee to communicate with us. 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.

8.2 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.

9.0 Contact details

If you have any questions about this Privacy Notice or about how we process your personal data, please contact us in the following way:

- Email address: dpo@augmentia.ai

10.0 Complaints

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK regulator for data protection issues (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.

11.0 Changes to the Privacy Notice and your duty to inform us of changes

We keep our Privacy Notice under regular review. This version was last updated in 01.09.2025 .
It is important that the personal data we hold about you is accurate and current.Please notify your GP of changes to your personal data.

12.0 National Data Opt-Out (UK)

As a data processor, Augmentia does not manage national data opt-outs. This responsibility lies with the data controller (e.g., your GP practice). Furthermore, at this time, our product does not share any personal data for planning or research purposes for which the national data opt-out would apply. We review all of the confidential patient information we process on an annual basis to see if this is used for research and planning purposes. If it is, then individuals can decide to stop their information being shared for this purpose. You can find out more information at https://www.nhs.uk/your-nhs-data-matters/