

Arcturis Real World Data Network: Transparency and Privacy Notice

Last updated: 11/11/2024 | This notice was co-developed with patients and members of the public. Our thanks to them for their time, generosity, and support.

This transparency and privacy notice provides detailed and technical information on how and why different types of data are processed by Arcturis Data (UK) Limited (“Arcturis”, “we”, or “us”) through our Real World Data Network (“RWD Network”).

For a more high-level overview of the RWD Network, please visit our Information for Patients and the Public webpage

The different types of data detailed in this notice are:

- **Patient personal data:** Information that relates to an identified or identifiable patient.
- **Anonymised clinical data:** Clinical data which does not relate to an identified or identifiable individual, or has been rendered anonymous in such a way that individuals are not (or are no longer) identifiable.

This notice is separated into sections. Each section provides key information initially followed by supplementary detail. If after reading this notice you have any questions or queries, or would like any further information, please do not hesitate to contact our Data Protection Officer by emailing dpo@arcturisdta.com

Information on how we process personal data for interventional medical research is provided separately (e.g. in study-specific Participant Information Sheets).

For information on how we process personal data collected for purposes other than public benefit medical research (e.g. through our website) please see our Privacy Policy.

Contents

Purpose for Processing Data	3
Lawful Basis for Processing Data	3
Categories and Sources of Data Processed	4
Recipients of Data	5
How Long Data is Retained For	5
How Data is Kept Confidential and Secure	6
Individual Rights relating to Patient Personal Data	6
The Right to Lodge a Complaint	7
Glossary of Terms	8

Purpose for Processing Data

- Patient personal data and anonymised clinical data are used for the purpose of conducting medical research which is of benefit to the public.
- Patient personal data remains within the NHS and only processing which is necessary to select, extract and anonymise clinical data is undertaken.

Our purpose for processing patient personal data and anonymised clinical data is to conduct medical research which is for public benefit. When this is undertaken through the RWD Network, this is limited to observational research using anonymised clinical data.

Observational research involves watching and recording events or phenomena without actively influencing or manipulating them. In the type of research Arcturis does, this is done by analysing anonymised clinical data to find the events or occurrences which can help develop or discover new treatments and medicines.

To ensure this research can lead to public benefit, we check and assure that:

- a) The public at large or a subset of the population (i.e. a particular patient group) would benefit from the research;
- b) The nature of that benefit is clear (e.g. lead to the identification or improvement of treatments) and is likely to materialise, and;
- c) Risks to the public arising from the research are identified and appropriately avoided or managed.

Lawful Basis for Processing Data

- When the processing of patient personal data is the legal responsibility of Arcturis, it is done as part of our legitimate interests as a commercial research consultancy for the purpose of research in the public interest.
- The NHS Health Research Authority has granted legal support for NHS staff who do not provide direct care to process confidential patient personal data without patient consent so only anonymised clinical data is shared with the RWD Network, following advice from the Confidentiality Advisory Group.

There may be occasions where the processing of patient personal data is the legal responsibility of Arcturis, even if the data and processing remain within another organisation. When this occurs, it is important Arcturis has lawful bases to process this information. Lawful bases are required under both UK data protection legislation and common law.

Under UK data protection legislation, our legal basis and conditions for processing are:

- **Legitimate Interests (UK GDPR Article 6[1][f]):** The processing is necessary for the purpose of the legitimate interests of Arcturis, these being to conduct business activity as a clinical research consultancy.
- **Research Purpose in the Public Interest (UK GDPR Article 9[2][j]).**

The NHS Health Research Authority has granted legal support for the Common Law Duty of Confidentiality to be temporarily lifted under Regulation 5 of the Health Service (Control of Patient Information) Regulations 2002 so trust staff who do not provide direct care can process confidential patient information without patient consent, so only anonymised clinical data is shared with the Arcturis Real World Data Network. Support has been given following advice from the Confidentiality Advisory Group.

Categories and Sources of Data Processed

- Patient personal data is information which can identify an individual and may include sensitive information. Arcturis does not request this category of data as part of the RWD Network, but it may be processed by NHS organisations in order for anonymised clinical data to be provided.
- The source of patient personal data processed for the Arcturis RWD Network are NHS organisations.
- Anonymised clinical data is information which has been made non-identifiable when processed by Arcturis.
- The source of anonymised clinical data include NHS organisations, health registries and academic institutions in the UK and from around the world.

There are two broad categories of data processed as part of the Arcturis RWD Network; 'patient personal data' and 'anonymised clinical data'.

Patient personal data is information which can identify a patient, such as name, address, and NHS number. This information will also include 'Special Category' data which relates to or infers a patient's race and ethnicity, religion, genetic information, sex life or sexual orientation, and health.

Arcturis does not request this category of data as part of the RWD Network. Instead, it is processed by NHS organisations who have entered into a data sharing agreement with Arcturis. These NHS organisations may process patient personal data in order to select, extract and anonymise the clinical data necessary for Arcturis to conduct observational research.

Anonymised clinical data is information which does not relate to an identified or identifiable individual or has been rendered anonymous in such a way that individuals are not (or are no longer) identifiable. This data will include information regarding race and ethnicity, religion, genetic information, sex life or sexual orientation and health but in a non-identifiable format (e.g. name and NHS number is removed, dates of birth and admission are altered etc.).

The Arcturis RWD Network processes and receives anonymised clinical data from a variety of sources. These will typically be from NHS organisations following the anonymisation of patient personal data, but also include non-NHS organisations, health registries and academic institutions in the UK and from around the world.

Recipients of Data

- No patient personal data is requested by the Arcturis RWD Network. Only anonymised clinical data is requested.
- Access to the anonymised clinical data made available to Arcturis is limited to only the RWD Network Team.
- Research findings and insights gained from anonymised clinical data are shared with clients, in scientific journals and at conferences.

Arcturis does not request access to patient personal data as part of the RWD Network, only anonymised clinical data.

Typically, only Arcturis engineering, informatics and research teams have access to this data. There may be limited circumstances where other Arcturis members of staff who support the RWD Network require access to the data. This is tightly controlled and on a 'need to know' basis.

Research findings and insights gained following the analysis of anonymised clinical data are shared with Arcturis clients. These may also be published in scientific journals and presented at conferences.

How Long Data is Retained For

- Patient personal data is processed only for as long as necessary.
- Anonymised clinical data is retained for as long as permitted by data sharing agreements.

Although Arcturis does not request patient personal data, the processing of it by NHS organisations is limited only to what is required to successfully select, extract and anonymise clinical data for the RWD Network.

All anonymised clinical data is shared with Arcturis under a contractually-binding data sharing agreement. These agreements specify the length of time Arcturis may retain this data and the circumstances of when access is revoked. As far as possible, Arcturis will seek to retain this data for as long as possible to support the needs of medicine and drug development and discovery research. It is not unusual for this to be more than 25 years.

How Data is Kept Confidential and Secure

- The Arcturis RWD Network only uses anonymised clinical data.
- Arcturis meets the standards of data security and protection required by the NHS.
- Wherever possible and practicable, Arcturis uses Privacy-Enhancing Technologies (PETs) to analyse data without it leaving the organisation that has provided it.
- Arcturis protects all anonymised clinical data received to best practice UK and international standards.

To help ensure patients are protected from harm, patient personal data is anonymised before it is made available to Arcturis for use as part of the RWD Network. The anonymisation process includes removing and changing data, and implementing legal restrictions and information security controls, so clinical data cannot be used to identify patients.

Arcturis meet the standards of data protection and information security required by the NHS. This is measured and assured through the NHS Data Protection and Security Toolkit (DSPT) which each organisation that processes patient data must complete annually. Results from the Arcturis NHS DSPT are available here: <https://www.dsptoolkit.nhs.uk/OrganisationSearch/8K382>.

Wherever possible and practicable, Arcturis uses Privacy-Enhancing Technologies (PETs) to analyse data without it leaving the organisation that has provided it. These PETs include:

- **Federated Analysis:** Analytical code is run against a data provider's database server(s) containing the clinical data, with only aggregated statistics and insights returned to Arcturis.
- **Secure Data Access:** Secure access to clinical data is given via a Secure Data Environment (SDE) and only aggregated statistics and insights are released to Arcturis.

Where the use of PETs is not appropriate, anonymised clinical data shared with Arcturis is protected to best practice standards of information security. These include to certification against the International Organization for Standardization's Information Security Management System (ISO27001) and UK Cyber Essentials standards.

Individual Rights relating to Patient Personal Data

- Patients in England have the right to 'opt-out' of having personal data about them shared for research. This can be done by registering a National Data Opt-Out by visiting <https://www.nhs.uk/your-nhs-data-matters/>.
- Patients can also request to exercise a number of rights afforded to them by UK data protection legislation. Due to the public interest research purpose for processing patient personal data, it may not always be possible to exercise these rights.
- Once patient personal data has been anonymised, these rights do not apply.

Patients have several rights which they can exercise in respect of personal data about them.

Patients in England are free to 'opt-out' of personal data about them being used for research – including by the Arcturis RWD Network - by registering a National Data Opt-Out. Further information, and the means to do this, is provided under the 'Ensuring patients have control – Opting-out and more' section of our Information for Patients and the Public webpage.

NHS organisations who process patient personal data for the RWD Network may also implement a RWD Network-specific opt-out. This allows patients to opt-out from having personal data about them being processed for the RWD Network but keep it available for other research initiatives. NHS organisations make the relevant patient population aware of this option.

Under UK data protection legislation, patient's also have the following rights:

- The right to request access.
- The right to request correction.
- The right to request erasure.
- The right to object to the processing.
- The right to request that the processing of your data is restricted.
- Request the transfer of your data to another party.
- Rights in relation to automated decision making and profiling.

Further information on these rights is available from the Information Commissioner's Office here:

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/>

Due to the public interest research purpose for processing patient personal data, it may not always be possible to exercise some of these rights.

It is important to note that once patient personal data has been anonymised (i.e. it becomes anonymised clinical data), 'opt-out' and data protection rights do not apply.

The Right to Lodge a Complaint

- Individuals with any questions, concerns or complaints are encouraged to contact Arcturis in the first instance through our Contact Us webpage.
- In respect of patient personal data, individuals have the right to lodge a complaint with a data protection supervisory authority. In a UK context, this is the Information Commissioner's Office.

If individuals have any questions, concerns or complaints regarding how Arcturis process data through the RWD network, they are encouraged to contact Arcturis in the first instance through our Contact Us webpage.

Where a complaint relates to the processing of patient personal data, individuals have the right to lodge a complaint with a data protection supervisory authority. In the UK, this is the Information Commissioner's Office (ICO). Information on how to complain to the ICO is provided through the following webpage: <https://ico.org.uk/make-a-complaint/>

Glossary of Terms

Term	Meaning
Anonymisation	The process of rendering identifiable data anonymous.
Anonymised clinical data	Clinical data which does not relate to an identified or identifiable individual, or has been rendered anonymous in such a way that individuals are not (or are no longer) identifiable.
Clinical Data	Information about people's health, care, or treatment, typically stored in hospital or GP records.
Confidentiality Advisory Group	An independent body which provides expert advice on the use of confidential patient information.
DSPT	Data Protection and Security Toolkit
Federated Analysis	A method of extracting insights from data on different systems without requiring the data to be brought to a central location.
Health Research Authority	The UK's national authority for regulating health research involving NHS patients and staff.
Informatics	The study of computational systems, focused on transformation of information.
National Data Opt-Out	A service in England that enables the public to register to opt out of their Confidential Patient Information being used for purposes beyond their individual care and treatment.
Patient personal data	Information that relates to an identified or identifiable patient.
Privacy-Enhancing Technologies (PETs)	Technologies that embody fundamental data protection principles by minimising personal data use, maximising data security, and/or empowering individuals.
'Section 251' support	A phrase that represents support provided under the Health Service (Control of Patient Information) Regulations 2002. Section 251 allows the common law duty of confidentiality to be lifted temporarily to enable disclosure of confidential patient information for medical purposes.
Secure Data Environment(s)	Data storage and access systems which allows approved users to access and analyse data without the data leaving the environment.