GDPR COMMITMENT

INTRODUCTION

The General Data Protection Regulation (GDPR) became effective May 25, 2018, providing a significant update to the law governing how personal data is collected and used, extending broader rights and control to individuals over how their personal data is processed while placing enhanced obligations on organizations processing personal data.

This statement explains our strong commitment to complying with the GDPR and provides some context to processing of personal data by iRhythm.

OUR COMMITMENT

iRhythm takes data privacy and security seriously. We have enhanced and continuously review our robust compliance program to further align with the unique elements of the GDPR. Our cross-functional project team, including external experts in security and data privacy, works with the focus of ensuring compliance and transparency with our customers and patients.

GDPR COMPLIANCE

As part of our GDPR preparation, we undertook a detailed analysis of all business processes where personal data is collected and used. We mapped our data flows and conducted a gap analysis against which we structured our compliance program. Key steps we have taken as part of this program include:

- Transparency
    - Reviewing and updating our privacy notices to physicians, patients, users of our website and our ZioReports portal, as well as communicating information about our lawful processing to meet our GDPR notification obligations.
- Processing Record
    - Documenting our records of personal data processing and determining and recording the appropriate lawful bases for each processing purpose. This is a living record that we keep under review.
- Subject Rights
    - Updating enhanced rights notices to individuals and implementing new and amended policies and processes to anticipate, manage and respond to the exercise of data subject rights.
- Security
    - Patient and Personal data is encrypted in transit and at rest. iRhythm's encryption policy meets or exceeds all generally accepted commercial and government standards.
- Incident Response
    - Reviewing and enhancing our existing incident response procedures to identify, investigate, contain and make all necessary reports within GDPR required time frames.
- Data Protection Impact Assessments (DPIAs)

- iRhythm has implemented a DPIA procedure and will conduct DPIAs where our processing of personal data is likely to result in a high level of risk. We have implemented processes to record each assessment and, where appropriate, to record and manage the measures to reduce the level of risk.

- Privacy by Design and Default
  - Developing guidance for use by product and systems developers so that iRhythm can seek to incorporate privacy by design and by default into new systems and processes.
- Policies and Procedures
  - Reviewing, updating and writing new policies and procedures to meet our enhanced GDPR obligations.
- Contracts
  - Requesting information as to the GDPR readiness of our service providers and conducting ongoing reviews and updating agreements relevant to personal data processing in line with GDPR requirements with clients and sub-contractors.
- Data Retention
  - Retaining personal data for the length of your use of the Zio service and as necessary to meet our contractual obligations, to identify issues or to resolve legal (or regulatory) proceedings. We may also retain aggregate information beyond this time for research purposes and to help us develop and improve our services. Patients cannot be identified from aggregate information retained or used for these purposes.
- Training and Awareness
  - Updating training materials and implementing a programme of training for employees on the requirements of the GDPR, raising awareness and further enhancing the culture of compliance within iRhythm.
- Privacy Official
  - We have designated ownership for privacy compliance within iRhythm. The Official is supported by a cross-functional team promoting awareness of the GDPR across the organisation.
- Notification
  - Our privacy policies can be viewed on our website at https://www.zioreports.com/Application.html#PP.
- Controller/Processor
  - Establishing that iRhythm is a controller and not a processor. As a controller, iRhythm understands that it is subject to the broader scope of obligations arising under data protection law to which its accounts are also subject.
- Accountability
  - Introducing systems and logs to capture and keep records of compliance measures taken.

iRhythm understands that continuous oversight and employee awareness are key to ongoing compliance with the GDPR. We continue to review personal data processing, adjusting and adapting our documentation as required.

If you have any further questions about our GDPR compliance, please contact us at UKprivacy@irhythmtech.com.