1.3.7 GDPR Article 28 Compliance

The items in this section define the responsibilities and liabilities of the Processor and the Controller as defined in GDPR article 28 section 3

CORE CONTENT IN SECTION 28

1. the subject matter of the processing

Establishing the eligibility of patients to take part in the Study

2. the duration of the processing

Until the end of the Study

3 and 4. the nature and the purpose of the processing

To establish the eligibility of individual patients to participate in the Study and, for patients consenting to join the Study, to maintain a flow of approved clinical data to the Study database.

5. the type of personal data involved

All patients with estimated GFR and proteinuria records in their history (Strategic Reporting Tables as defined in the Data Sharing Agreement 1.3.8). This includes all coded history and medication history and demographic details.

6. the categories of data subjects

All patients with Estimated GFR and proteinuria criteria used to identify potential adult participants with CKD.

7. the controller's obligations and rights

The Controller is responsible for the GDPR compliance of the Processor they use to process their data. The Processor has a duty to inform the Controller of any data breach without undue delay.

ELEMENTS SPECIFICALLY PROVIDED FOR IN SECTION 28

(a) the processor must only act on the controller's documented instructions, unless required by law to act without such instructions

This Data Sharing Agreement includes the instruction from the Data Controller to process the data for the purpose set out in this Data Sharing Agreement (1.3.6).

(b) the processor must ensure that people processing the data are subject to a duty of confidence

TCR (Nottingham) Ltd contracts of employment include a duty of confidentiality.

(c) the processor must take appropriate measures to ensure the security of processing

The Data Security and Protection (DSP) Toolkit sets out the framework for securely managing and processing patient data. TCR (Nottingham) Ltd have successfully completed this toolkit and the results (rated Satisfactory) are available to view online. TCR's registration number is 8HP44. All data is held either in the practice on a designated PC or on hosted servers within N3/HSCN. Demographic data is encrypted at rest to AES256 standard. Secure backups are maintained to allow timely recovery in the event of a physical or technical incident. Servers are maintained by Nottinghamshire Health Informatics in their UK data centre. Penetration testing

is carried out periodically on servers. Processes are reviewed periodically as part of the DSP Toolkit conformance processes.

(d) the processor must only engage a sub-processor with the controller's prior authorisation and under a written contract

There are no sub-processors associated with this Data Sharing Agreement.

(e) the processor must take appropriate measures to help the controller respond to requests from individuals to exercise their rights

All data held for individual patients is available for the Data Controller on request. Any requests received by TCR (Nottingham) Ltd will be passed to the Data Controller without undue delay.

(f) taking into account the nature of the processing and the information available, the processor must assist the controller in meeting its UK GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments

Reference DSP Toolkit section 6. A mechanism for reporting data breaches is in place.

TCR (Nottingham) Ltd will assist the Controller in meeting its UK GDPR obligations

A TCR Data Protection Impact Assessment (DPIA) is available for the ATTACK Study. A DPIA for the Study is available from the ATTACK Study Clinical Trials Manager.

(g) the processor must delete or return all personal data to the controller (at the controller's choice) at the end of the contract, and the processor must also delete existing personal data unless the law requires its storage

All data held by TCR (Nottingham) Ltd for patients will be deleted in a secure manner at the end of the Study. The practice will be removed from the data extraction process to prevent any further data flow.

Data for consented patients held in the Study database will be retained in line with the Attack Study Protocol.

(h) the processor must submit to audits and inspections. The processor must also give the controller whatever information it needs to ensure they are both meeting their Article 28 obligations.

TCR will submit to audits and inspections and provide the controller with whatever is needed to ensure Article 28 obligations are being met.

Signed Clive Morris – Managing Director TCR (Nottingham) Ltd

JUNE 8th 2022