G1 Therapeutics, Inc. TECHNICAL AND ORGANISATIONAL MEASURES
Effective as of 27 December 2022

G1 Therapeutics, Inc. takes appropriate organizational and technical measures (processes, controls, systems and procedures) to protect the security, confidentiality, accuracy, integrity, and availability of Protected Data. Such measures include at a minimum:

Organizational Measures

- Security Policy(ies) which address access, asset management and password controls.
- Business Continuity Plan or equivalent describing how data is secured, accessed, recovered and maintained in the event of an incident.
- Data Protection Policy and Procedures available to its employees as a form of guidance and support.
- Incident Response Plan which outlines processes and procedures for managing a Personal Data Breach (when a breach of security leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed). This Incident Response Plan shall be compliant with the requirements of GDPR in respect of data breach management and reporting.
- Awareness & Training – ensuring employees and contractors understand Vendor's data protection obligations, including training and support.
- Hold staff with access to personal data accountable for maintaining confidentiality obligations.
- Vendors shall have in place a procedure to allow them to respond to data requests as defined in the GDPR.
- Reviews & Audits – auditing functions, activities and systems to evidence that policies and controls are followed.
- Due Diligence – ensuring employees suppliers and subcontractors are able to fulfil the same requirements with regard to Regulation and data protection laws.

Technical Measures

- Identity and Access Management - Vendor shall have proper identity and access controls in place to restrict access to personal data to authorized personnel to ensure that they have access only to information or systems applicable to their job function. Only those who need access to personal information to perform their job have access. Vendor will have adequate password strength and

use multi-factor authentication (MFA) where possible. MFA is mandatory for remote access to sensitive information.

- Privacy training will be provided to those individuals to ensure that the intended purpose for the collection of personal data is maintained.

- Physical Security - protecting any office or building from unauthorized access by limiting physical access to secured areas (e.g., visitor sign-in, security cameras, card access readers, and/or physical keys, ID badges).

- Cyber Security – including firewalls, malware scans, anti-virus protection, intrusion detection and response systems, endpoint detection and response systems (or similar).

- Encryption & Pseudonymization - Vendor shall process any personal data using encryption and pseudonymization using field level encryption in databases, encryption of entire data stores at rest, as well as encryption for data in use and in transit.

- Regular penetration testing is performed to ensure the network security posture is effective.

- Back-ups: Vendor shall have off-site back-up procedures in place including regular restoration testing.

- Data Loss Prevention – implementation of processes and procedures to preserve data stored by the Vendor in the event of damage or failure to computer systems or their components.

- Disposal – adequate and compliant disposal of paperwork and devices (e.g., shredding and certified disposal of hard-copy records and policies and procedures for disposal of electronic data.