RHAPSODY DATA PROTECTION AND SECURITY STANDARDS

As part of Rhapsody's commitment to the protection of Customer Personal Data, Rhapsody has established its information security requirements for its solutions as outlined in this Rhapsody Data Protection and Security Standards Exhibit ("Security Exhibit"). The Security Exhibit shall be effective as of the date Rhapsody first receives, maintains, transmits, accesses or otherwise comes into contact with Customer Personal Data. The requirements are intended to describe the minimum standard for physical, technical, and administrative controls affecting Customer Personal Data in relation to the services Rhapsody has been retained to provide by the Customer as per the underlying Agreement between Rhapsody and the Customer.

1. DEFINITIONS

"Agreement" means the underlying agreement for products and/or services entered into between Rhapsody and the Customer of which this Security Exhibit forms a part.

"Customer" means the party, other than Rhapsody, identified in the Agreement.

"**Customer Personal Data**" includes all data provided by or generated for Customer including, but not limited to Customer Personal Data, Protected Health Information ("PHI" as defined under HIPAA), and other regulated and confidential information.

"Data Protection Laws" mean (a) the applicable national, state, local or other data privacy law or statute identified as the Jurisdiction in the Agreement; (b) any applicable data privacy related international or transnational treaty, law, or statute; and (c) any applicable data privacy rule or regulation issued by a governmental regulatory body having jurisdiction over the activities contemplated by this agreement.

"EU Personal Data" means Personal Data related to individuals residing in the European Union or the United Kingdom.

"GDPR" means the General Data Protection Regulation (EU) 2016/679

"Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, unsecured personal data, including PHI or PII, transmitted, stored or otherwise processed.

"Personnel" includes Rhapsody's employees, contractors, subcontractors, and any other persons who have access to the Customer's facilities, systems, or Customer Personal Data.

"**Process**" or "**Processing"** means performing any operation or set of operations on Customer Personal Data whether or not by automated means such as collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

"**Rhapsody**" means the Rhapsody entity or entity(ies) named in the Agreement providing products and/or services to the Customer, together with its affiliate companies.

"Security Program" means the privacy and security policies and procedures maintained by Rhapsody as defined in Section 3 (Security) of this Security Exhibit.

"**Services**" means the services supplied by Rhapsody under the Agreement which shall involve the processing of Customer Personal Data on behalf of Customer.

2. PRIVACY AND DATA PROTECTION

a. Rhapsody agrees to comply with all applicable Data Protection Laws when providing its Services to the Customer.

b. Rhapsody shall:

   i. Process Customer Personal Data only in accordance with documented instructions from the Customer;

   ii. Take all reasonable steps to ensure the reliability and integrity of any Personnel or other authorized contractors or agents who have access to Customer Personal Data and ensure that the Personnel are aware of and have committed themselves to appropriate confidentiality obligations based on the type of data the Personnel are handling and that they have undergone adequate training in the use, care, protection and handling of Customer Personal Data;

iii. Ensure that at all times Rhapsody has in place appropriate technical and organizational measures to guard against unauthorized or unlawful Processing of the Customer Personal Data and/or accidental loss, destruction or damage to the Customer Personal Data in accordance with the requirements of Data Protection Laws, including without limitation the measures described in Section 3 (Security) and any additional security measures documented in the Agreement between the parties;

iv. Not disclose, make available or transfer Customer Personal Data to any subcontractor or other third party without the express prior written authorization of the Customer.

v. not Process or allow for the Processing of any Customer Personal Data outside the country where the customer is located unless otherwise agreed to by the parties.

vi. Procure that any authorized sub-contractor or other third party who will be processing or accessing Customer Personal Data enters into a data processing agreement with Rhapsody on terms which are equivalent to those in this Section b;

vii. Taking into account the nature of the processing, assist the Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of any obligation on the Customer to respond to requests for exercising the rights available to individuals under Data Protection Laws, including notifying the Customer within 10 business days and providing full details and copies of complaints or requests it receives from an individual or from a data protection regulator and provide on request by the Customer, with any Customer Personal Data it holds in relation to the individual;

viii. Make available to the Customer all information necessary to demonstrate compliance with its obligations in this Security Exhibit, and allow for and contribute to audits, including inspections, conducted by the Customer or a third-party auditor mandated by the Customer in accordance with clause 15;

ix. at the choice of the Customer, delete all Customer Personal Data after the end of the provision of services, and delete existing copies unless applicable laws require storage of the Customer Personal Data; and

x. use all reasonable endeavors to assist the Customer to comply with its obligations under applicable Data Protection Laws and not perform its obligations under this Security Exhibit in such a way as to cause the Customer to breach any of the Customer's obligations, to the extent Rhapsody is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

c. To the extent Rhapsody will process EU Personal Data as part of the Services, the parties may choose to enter into additional General Data Protection Regulation terms. In addition to any such terms in the Agreement:

i. Rhapsody shall be deemed the Processor, and the Customer shall be deemed the Controller for the purposes of the "GDPR, unless otherwise stated in the Agreement between the parties;

ii. Rhapsody shall not process any EU Personal Data in any country outside the European Economic Area without the express prior written authorization of the Customer, except to extent authorized in the Agreement; and

iii. Rhapsody shall assist the Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 of GDPR taking into account the nature of processing and the information available to the ***Rhapsody.***

d. To the extent Rhapsody will Process protected health information subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (US), the parties shall execute a Business Associate Agreement.

3. **SECURITY**

a. **Security Program Requirements**. Rhapsody shall maintain a comprehensive Security Program that has the physical, administrative, and technical safeguards to: (i) ensure the security and confidentiality of Rhapsody Data; (ii) protect against threats/hazards to the security of the Customer Personal Data, (iii) protect against any unauthorized use of or access to Customer Personal Data, and (iv) protect the integrity of Customer Personal Data. The Security Program shall be no less rigorous than those maintained by Rhapsody for its own data and information of a similar nature; shall be based on known industry standards (e.g., ISO 27001, NIST); and shall ensure compliance with Data Protection Laws such as the Health Information Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH) and the GDPR (as applicable).

b. **Security Program, Policy and Procedures Updates**. Rhapsody shall update its Security Program, policies and procedures as necessary to comply with changes in applicable federal, state, and local laws and regulations and meet the standard of due care/diligence, pertaining to the privacy and protection of Customer Personal Data. Upon request, Rhapsody shall review with the Customer its policies and procedures.

c. **Subcontractors**. In the event Rhapsody utilizes any subcontractors Rhapsody shall exercise due diligence involving subcontractors performing services related to Rhapsody and/or who have access to Customer Personal Data, applications, or systems to ensure they comply with requirements in this Security Exhibit. Rhapsody shall employ a comprehensive Third-Party Vendor Management Policy to evaluate, document, and remediate risks associated with Third Party relationships. Rhapsody shall include substantially similar terms and conditions as specified in this Security Exhibit in all contracts and subcontracts related to the provision of services to the Customer, and as otherwise required by Data Protection Laws.

d. **Breach Response and Reporting**. Any reported Breach is any event that impairs the security of unsecured Customer Personal Data including any (i) unauthorized access, use, disclosure, modification, or destruction of Customer Personal Data; or (ii) act that violates applicable privacy laws (including Data Protection Law) or any Rhapsody security policy. If Rhapsody detects a Breach, Rhapsody shall:

    i. Unless otherwise agreed to by the parties, notify the Customer promptly and no later than seventy-two (72) hours after Rhapsody becomes aware of a security Breach involving unsecured Customer Personal Data.

    ii. Immediately perform incident management actions as appropriate, including, but not limited to: responding, investigating, collecting, analyzing and preserving evidence; containing, remediating and mitigating adverse impacts; remediating, recovering, etc., all as related to the Breach.

    iii. If requested by the Customer, prepare and deliver to the Customer within five (5) business days of the confirmed security Breach a root cause report that describes in detail (i) a description of the nature and extent of the Breach; (ii) the unsecured Customer Personal Data altered, disclosed, destroyed, or otherwise compromised; (iii) all supporting evidence, including system, network, and application logs related to the Breach; (iv) all investigative, corrective and remedial actions completed, and planned actions and the dates by which such actions will be completed; and (v) all efforts taken to mitigate the risks of further Breaches.

e. **Security Assessments**. Rhapsody's Security Program shall facilitate the regular assessment of risks and vulnerabilities that may be present in the Services.

f. **Annual Penetration Testing**. Rhapsody will, at its own cost, engage an independent third party to perform penetration testing and vulnerability assessment of the Services, systems, or applications at least annually, and provide a summary of results to Rhapsody upon request.

g. **Security Vulnerability Remediation**. Based on the security testing and assessment results, remediation of findings shall be prioritized and applied based on risk and criticality of the vulnerabilities. Rhapsody shall mitigate any Critical or High-risk vulnerabilities within 14 days of the remediation (security patch) being available.

h. **Right to Audit**. During the term of the Agreement and not more than once per year (unless circumstances warrant additional audits as described below), the Customer may audit Rhapsody security, privacy, and compliance policies, procedures upon at least thirty (30) days' notice at a mutually convenient time to Rhapsody and the Customer. Notwithstanding the foregoing, the parties agree that the Customer may conduct an audit at any time, in the event of audits required by the Customers' governmental or regulatory authorities.

i. **Background Checks and Training**. Prior to assigning any Personnel to positions in which they are reasonably expected to have access to Customer Personal Data, Rhapsody and its subcontractors, agents, etc., will conduct background checks and ensure all individuals are trained with respect to Rhapsody's security policy and procedures.

j. **Account and Password Requirements**. Each Personnel must have an individual account that authenticates the individual's access to Customer Personal Data or systems. Rhapsody will not allow sharing of accounts. The Services will adhere to strong password requirements (minimum 10 characters, at least one character from each of the four-character sets, 90-day expiration (60 for privileged accounts), and no reuse of the previous 6 passwords).

k. **Access and Authorization**. Rhapsody will employ physical and logical access control mechanisms to prevent unauthorized access to Rhapsody facilities and systems associated with Customer Personal Data, applications, and systems and shall limit access to Personnel with a business need to know. Such mechanisms will have the capability of detecting, logging, and reporting access to the system or network or attempts to breach the security of the facility, compartment, system, network, application, and/or data. Without limitation:

    i. Rhapsody will utilize multi-factor authentication for privileged accounts.

    ii. Rhapsody will maintain a process to review access controls at least annually for all Rhapsody Personnel. Rhapsody shall revoke access for any Personnel who no longer have a need for such access. Rhapsody will maintain the same processes of review and validation for any third party hosted systems it uses.

    iii. Rhapsody will revoke Personnel's access to the Customer physical locations, systems, and applications within twenty-four (24) hours of the cessation of such Personnel's need to access the system(s) or application(s) or immediately if warranted or requested by the Customer.

l. **Secure Programming Techniques**. All application and system development shall follow industry best practices and processes for secure programming.

m. **Data Transmission and Storage**. Rhapsody shall not access, view, transmit or store Customer Personal Data, or allow its employees or agents to download, extract, store, or transmit Customer Personal Data through personally owned computers, laptops, personal digital assistants, tablet computers, cell phones, or similar personal electronic devices.

n. **Change Management**. Rhapsody will employ an effective documented change management program with respect to the Services delivery.

o. **Malicious Code Protection**. All Rhapsody managed workstations and servers must run anti-virus software. Virus definitions must be updated within twenty-four (24) hours. Real-time scanning of machines must occur in regularly scheduled intervals, not to exceed seven (7) calendar days. Rhapsody will scan incoming content for malicious code on all gateways to public networks including email and proxy servers.

p. **Data Encryption**. Rhapsody will utilize NIST-approved encryption algorithms and key strengths to encrypt Customer Personal Data when in transit, at rest in any application or system, or transported/stored via any physical media. Without limitation:

    i. If computers or mobile devices (e.g., desktops, laptops, mobile phones, tablets) are used to perform any part of the Services, Rhapsody will encrypt all Customer Personal Data on such mobile devices.

ii. Where encryption is utilized, Rhapsody will maintain a key management process that includes appropriate access controls to limit access to private keys (both synchronous and asynchronous) and a key revocation process. Private keys must not be stored on the same media as the data they protect.

q. **Physical Data**. Rhapsody shall not keep any Customer Personal Data in physical form unless required as part of providing the Services and is authorized by the Customer. Any hard copy or physical information will be destroyed at the completion of the contract unless required by law.

r. **Designated Security Representatives**. The following individual is Rhapsody's Security Representative. All notifications required under this Security Exhibit shall be made to this individual.

Rhapsody Security Representative:

Name: Sameer Sule
Title: CISO & VP, Compliance
Phone: 972-942-0270
E-mail: Sameer.sule@rhapsody.health