Lyfegen Terms & Conditions – Version 12.2.2024 (current, binding)

Lyfegen Terms & Conditions

1. **Scope**

1.1 These Lyfegen Terms & Conditions ("**LTC**") contain the general contractual terms and conditions applicable to the services provided by the Provider to the Customer in relation to the access and use of the Lyfegen Platform by the Customer, and the relationship of the Parties in general. The Work Orders govern the details of the Customer's subscription to the Lyfegen Platform and the SaaS Services and ancillary services to be provided by the Provider under these LTC and the Work Order. Each Work Order shall, upon its execution by the Parties, be governed by the provisions of these LTC and the additional provisions set forth in the Work Order. Where the Parties enter into several successive Work Orders under the LTC, the version of the LTC of the most recent Work Order entered into by the Parties shall apply to such Work Order and shall take precedence over all versions of the LTC agreed under previous and ongoing Work Orders, (a) unless provided otherwise in the latest Work Order or (b) unless the Provider amends these LTC in accordance with Section 20 and the Customer does not timely object. All ongoing Work Orders together, the applicable LTC (as amended from time to time as per further Work Orders or other agreement between the Parties) and the applicable annexes form one coherent contract ("**Agreement**"). Any general terms and conditions of the Customer do not apply between the Parties under the Agreement, even if expressly referred to in an order document issued by the Customer.

1.2. The terms and annexes of these LTC, as listed below or agreed later on, shall be deemed to be part of the Agreement.

1.2.1. Applicable terms and annexes of these LTC for the Customer acting as a HPP, as specified in the Work Order:

- LYFEGEN TERMS & CONDITIONS, except Sections 3.3 , 12.3 and 12.4.
- ANNEX 1: FUNCTIONAL DESCRIPTION OF THE LYFEGEN PLATFORM AND ANCILLARY SERVICES
- ANNEX 2: SECURITY
- ANNEX 3: SUPPORT AND SERVICE LEVEL
- ANNEX 4: PROCESSING OF CUSTOMER DATA AND OTHER PERSONAL DATA
- ANNEX 5: LYFEGEN PLATFORM DATA PROCESSING ADDENDUM
- ANNEX 5A: SUBPROCESSORS
- ANNEX 5B: TECHNICAL AND ORGANIZATIONAL MEASURES OF SECURITY

1.2.2. Applicable terms and annexes of these LTC for the Customer acting as a Supplier, as specified in the Work Order:

- LYFEGEN TERMS & CONDITIONS, except Sections 3.2, 5.1, 12.2 and 12.4
- ANNEX 1: FUNCTIONAL DESCRIPTION OF THE LYFEGEN PLATFORM AND ANCILLARY SERVICES
- ANNEX 2: SECURITY
- ANNEX 3: SUPPORT AND SERVICE LEVEL
- ANNEX 5: LYFEGEN PLATFORM DATA PROCESSING ADDENDUM
- ANNEX 5A: SUBPROCESSORS
- ANNEX 5B: TECHNICAL AND ORGANIZATIONAL MEASURES OF SECURITY

1.2.3 Additionally, if applicable, as specified in the Work Order, the following HIPAA/HITECH changes apply to the applicable terms and annexes of these LTC according to Section 1.2.1 or Section 1.2.2, as applicable:

- LYFEGEN TERMS & CONDITIONS:
    - In Section 2: The definitions of the terms in 2.9, 2.12, 2.26 and 2.30 shall be those included for the purposes of the HIPAA/HITECH
    - Section 12.4 applies
- ANNEX 6: BUSINESS ASSOCIATE PROVISIONS applies

    1.3. To the extent any terms or provisions of a Work Order or any customer-specific amendments ("**Customer-Specific Amendment**") conflict with these LTC (including their annexes), these LTC and their annexes shall have precedence over the individual Work Order or Customer-Specific Amendment, except to the extent that the applicable Work Order or Customer-Specific Amendment states an intent to supersede these LTC on a specific matter. As a special rule, any specific agreement in a Work Order as to the features or functionalities of the Lyfegen Platform or services to be provided by the Provider shall have precedence over Annex 1 of the LTC.

    1.4. Where these LTC provide that certain provisions only apply to Customer acting as a HPP or as a Supplier, only those provisions corresponding to Customer's role shall apply. While Customer understands and accepts that its Contract Partner(s), in view of the manner in which the Lyfegen Platform is operated, have entered into, or may enter into, the same or similar terms for its own relationship with the Provider as did the Customer, it agrees that the Provider has no obligation to ensure so or make available to Provider its own agreements with the Contract Partner(s) of the Customer.

1. **Definitions**

2.1. "**Administrator**" means a User of the Customer who has increased privileges to manage the access to the Lyfegen Platform for the Customer's Users as per the Agreement. The initial User communicated by the Provider to Customer is always considered to be an Administrator, and so is any other User who has been given the "administrator" role by an Administrator within the Lyfegen Platform.

2.2. "**Agreements Module**" means the SaaS service provided using a cloud-based application as further defined in Annex 1.

2.3. "**All-Inclusive Mode**" means the combination of the Personal Data Mode and the Non-Personal Data Mode in the Data Module.

2.4. "**Data-Driven Contract**" means a particular value and data-driven agreement that has been agreed between two or more customers of the Provider and implemented by them within the Agreements Module using Lyfegen's own technology.

2.5. "**Data-Driven Contract Record**" means the data record produced by the Agreements Module for each Data-Driven Contract and to be provided to the Customer and its contractual partner(s) or designated Receiving Partners, as part of this Agreement, with such data record potentially containing Personal Data of patients, doctors, nurses and other medical personnel involved in the treatment of patients; the data fields used to generate the data record are defined in or pursuant to the individual Work Order at issue.

2.6. "**Receiving Partner**" means any individual with whom the Customer wants to share Data-Driven Contract Records and/or Financial-Driven Contract Records generated by the Agreements Module through the Sharing Module of the Lyfegen Platform. It does not matter whether the Receiving Partner has a contract with the Provider or not. Such Receiving Partner will be granted access to the Data-Driven Contract Records and/or Financial-Driven Contract Records selected by Customer through the Lyfegen Platform (e.g., by way of a link via e-mail); anyone who has the link as well as access to the relevant e-mail account can retrieve the content and communicate with the Customer via the Lyfegen Platform.

2.7. "**Contract Partner**" means the Supplier or HPP, with which the Customer has entered into or will enter into Data-Driven Contracts and/or Financial-Driven Contracts, as the case may be, that are to be implemented in the Provider's Agreements Module for the purposes of executing event or other data records received from the Data Module or financial data records, subject to such healthcare payers and providers or pharmaceutical manufacturers or other suppliers also having entered into the necessary corresponding SaaS subscription agreement with the Provider.

2.8. "**Controller**" means the natural or legal person that, alone or jointly with others, determines the purpose and means of the Processing of Personal Data; the term shall be interpreted in accordance with the GDPR.

2.9. "**Customer**" means the company mentioned as Customer in the relevant Work Order(s) executed by the Parties under these LTC; for the purposes of HIPAA (if applicable), Customer shall be the "Covered Entity" as that term is defined in such law.

2.10. "**Customer Data**" means all data, files, documents, audio and visual information, graphics or code in any form, format or media (including paper, electronic and other records) that the Customer creates, installs, uploads to or transfers in or through the Lyfegen Platform or provides in the course of using the Lyfegen Platform for the purpose of being Processed by the Lyfegen Platform, or is provided with for its own use through the Platform, including Personal Data of patients, doctors, nurses and other personnel involved in the treatment of patients, including any Data-Driven Contract Records of the Data-Driven Contracts to which the Customer is a party (after such Data-Driven Contract Records have been handed over by or to the Customer, as the case may be), but not including (a) Pricing Data and (b) data on Users as needed to manage access to, and use of the Lyfegen Platform, such as usernames, passwords, permissions and contact details of Users.

2.11. "**Data Module**" means the SaaS service provided using a cloud-based application as further defined in Annex 1.

2.12. "**Data Protection Legislation**" means Laws, which protect the privacy rights of individuals, insofar as they apply to the Processing of Personal Data in connection with this Agreement including without limitation and as may be applicable (a) the GDPR, any local, provincial or national legislation implementing the GDPR, (b) the Swiss Federal Act on Data Protection and the Swiss Ordinance on the Federal Data Protection Act, and (c) any corresponding or equivalent data protection legislation to which either Party is subject, including any local, state, provincial or national Laws implementing any such legislation and (d) HIPAA and HITECH (if applicable), in each case, any new or revised version of the foregoing from time to time.

2.13. "**Data Subject**" means a natural person whose Personal Data is Processed.

2.14. "**Financial-Driven Contract**" means a particular value and financial-driven agreement that has been agreed between the Customer and one or more contractual partners of the Customer (which may also be a customer of the Provider) and implemented within the Agreements Module using Lyfegen's own technology.

2.15. "**Financial-Driven Contract Record**" means the data record generated by the Agreements Module for each Financial-Driven Contract and to be provided to the Customer and its contractual partner(s) or designated Receiving Partners, as part of this Agreement; the data fields used to produce the data record are defined in the individual Work Order at issue.

2.16. "**Financials Module**" means the SaaS service provided using a cloud-based application as further defined in Annex 1.

2.17. "**HPP(s)**" mean healthcare payers (e.g., insurance companies) and providers (e.g., hospitals) under this Agreement, and, in the present context, any Customer who has been agreed to have the role of a HPP in the applicable Work Order (for the SaaS Services agreed therein).

2.18. "**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, and any new or revised version thereof from time to time.

2.19. "**HIPAA**" means the U.S. Health Insurance Portability and Accountability Act of 1996, and all regulations thereunder, in each case, any new or revised version of the foregoing from time to time.

2.20. "**HITECH**" means the US Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009, and all regulations thereunder, in each case, any new or revised version of the foregoing from time to time.

2.21. "**Law**" means any local, state, national and/or foreign law, treaties, and/or regulations applicable to a respective Party with respect to the SaaS Services contemplated in the Agreement.

2.22. "**Lyfegen Platform**" is the umbrella term used in the Agreement to refer to SaaS Services (and ancillary services, where applicable) as may be provided by the Provider to the Customer under this Agreement and the individual Work Orders, as further outlined in Annex 1.

2.23. "**Non-Personal Data Mode**" or "**NPD mode**" means the mode in the Data Module, which allows to register and manage Pricing Data, including financial data records of a particular medication, with such Pricing Data being Processed by the Agreements Module in connection with Financial-Driven Contract(s), excluding the registration and management of Customer Data.

2.24. "**Parties**" mean the Provider and the Customer (each a "**Party**") as mentioned in the relevant Work Order(s) executed by the Parties under these LTC.

2.25. "**Personal Data Mode" or "**PD mode**" means the mode in the Data Module, which allows to register and manage Customer Data, including event data records related to the treatment of individual patients, with such Customer Data being Processed by the Agreements Module in connection with Data-Driven Contract(s), excluding the registration and management of Pricing Data.

2.26. "**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; the term shall be interpreted in accordance with the GDPR; for the purposes of HIPAA (if applicable), Personal Data means any information that identifies or can be used to identify a natural person, including "protected health information" as defined in HIPAA or personal information regarding an identifiable natural person which is protected by applicable Law. Such Personal Data may include information: (i) provided to Lyfegen by Customer or (ii) obtained, used, accessed, Processed, possessed or acquired by Lyfegen on behalf of Customer or otherwise in connection with the provision of goods and/or services to or for Customer. For this purpose an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; the term shall be interpreted in accordance with the GDPR or other applicable Law.

2.27. "**Pricing Data**" means all data, files, documents, audio and visual information, graphics or code in any form, format or media (including paper, electronic and other records) containing financial data records of a particular medication that the Customer or any other authorized third party creates, installs, uploads to or transfers in or through the Lyfegen Platform or provides to the Provider in the course of using the Lyfegen Platform for the purpose of being Processed by the Lyfegen Platform, or is provided with for the Customer's own use through the Platform, such as purchase history, applicable discounts, caps, and other commercial aspects related to the price of the medication, and, as the case may be, information related to the effectiveness of the medication on individual patient treatments (without those patients being identifiable), as well as any Financial-Driven Contract Records of the Financial-Driven Contracts to which the Customer is a party, but not including data on Users as needed to manage access to, and use of the Lyfegen Platform, such as usernames, passwords, permissions and contact details of Users.

2.28. "**Processing**" or "**Processed**" means any operation or set of operations which is performed on Personal Data, on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; in the context of this Agreement, the term "processing" may also be used in connection with non-personal data.

2.29. "**Processor**" means the legal person that Processes Personal Data on behalf of a Controller; the term shall be interpreted in accordance with the GDPR.

2.30. "**Provider**" means the company mentioned as Provider in the relevant Work Order(s) executed by the Parties under these LTC; for the purposes of HIPAA (if applicable), Provider shall be the "Business Associate" as that term is defined in such law.

2.31. "**RefaaS**" is a refund as a service whereby the Provider assumes the task to collect, for and on behalf of the Customer (under a power of attorney), from Customer's Contract Partner(s) (acting as Supplier) all refunds that those Contract Partner(s) owe to Customer under the the Data-Driven and/or Financial-Driven Contracts implemented in the Agreements Module as per the information contained in the Lyfegen Platform. If the Customer wishes to restrict the service to certain categories of refunds, amounts or Contract Partner(s), this shall be agreed in the relevant Work Orders(s); by default, all categories of refunds, amounts and Contract Partner(s) as per the Lyfegen Platform shall be covered by and included in the service.

2.32. "**RefaaS Services**" shall mean the RefaaS services provided by the Provider to the Customer, as specified in Annex 1 and as selected and agreed upon by the Parties in the relevant Work Order(s).

2.33. "**Relevant Contract Record(s)**" means the Data-Driven Contract Record and/or the Financial-Driven Contract Record generated by the Agreements Module.

2.34. "**SaaS**" is a software as a service licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted on the server of a cloud service provider. It is sometimes referred to as "on-demand software".

2.35. "**SaaS Services**" shall mean the SaaS services provided by the Provider to the Customer under these LTC, including access to the Lyfegen Platform with the features, functionalities and modules as specified in Annex 1 and as selected and agreed upon by the Parties in the relevant Work Order(s).

2.36. "**Sharing Module**" means the SaaS service provided using a cloud-based application as further defined in Annex 1.

2.37. "**Section**" means any section of these LTC.

2.38. "**Start Date**" means the start date as agreed in the relevant Work Order.

2.39. "**Supplier**" means a pharmaceutical manufacturer or similar company under this Agreement, and, in the present context, any Customer who has been agreed to have the role of a Supplier in the applicable Work Order (for the SaaS Services agreed therein).

2.40. "**Third Party Products**" mean application software products provided by third party vendors, including operating system and application software with which the Lyfegen Platform interfaces and which provides certain functionality essential to the operation of the Lyfegen Platform. Third Party Products are licensed to the Provider for incorporation and use in the hosted environment as part of the Lyfegen Platform. For the sake of clarity, the term Third Party Products does not refer to third-party software components, if any, incorporated into the Lyfegen Platform.

2.41. "**Underlying Contract**" means the Data-Driven Contract and/or Financial Driven Contract that has been agreed between the Customer and the relevant Contract Partner. The Provider is not part of it.

2.42. "**User(s)**" means any individual, entity, role or system that directly or indirectly through another user accesses or uses the Lyfegen Platform through the access credentials provided to, or created by, the Customer, in particular its Administrators. Users can be the Customer's employees, representatives, consultants, contractors, agents or other roles who are authorized to use the Lyfegen Platform and have been supplied with user identifications and passwords by the Customer or on the Customer's behalf. Users can also be systems.

2.43. "**Work Order(s)**" means any written document or online order form made available by the Provider to the Customer through the Lyfegen Platform and agreed by the Parties under these LTC by way of signing or using an online process (including electronic signing services such as DocuSign or Adobe Sign or a process implemented on the Lyfegen Platform). Each Work Order details, inter alia and to the extent applicable, (a) the role of the Customer, (b) the Customer's subscription to the Lyfegen Platform, (c) the Provider's SaaS Services (and ancillary services, if applicable) to be provided, (d) any specific features and functionalities of the Lyfegen Platform that shall have precedence over Annex 1 of the LTC, and (d) the fees due by the Customer to the Provider for the SaaS Services and, where applicable, the ancillary services. A Work Order shall only binding upon the Provider if confirmed by it following Customer having agreed to it. See also Section 8.4.

1. **Provision of Services**

3.1. Subject to the conclusion of a corresponding Work Order, the Provider provides the Customer, for the term as per the relevant Work Order, access to the Lyfegen Platform, and shall provide the ancillary services, with the features and functionalities as further specified in Annex 1 and the relevant Work Orders, subject to Section 10 and the other provisions of these LTC, including the relevant Work Order.

3.2. Where the Customer acts as a HPP, as specified in the Work Order, the following applies:

3.2.1. As agreed in the relevant Work Orders, such access will cover access to the Data Module with the mode specified therein and/or the Agreements Module, each individually or together; in the case of the Agreements Module, such access will include access to the Data-Driven Contracts and/or the Financial-Driven Contracts, as the case may be, resulting from the value and data-driven agreements and/or the value and financial-driven agreements that the Customer has agreed with its contractual partner(s) (which may also be customer(s) of the Provider).

3.2.2. The Customer acknowledges and accepts that with regard to such Underlying Contracts, (a) the Provider is not party to the Underlying Contracts or other cooperation agreements between the parties to such Underlying Contracts, and (b) that any issue, controversy, claim or other dispute related thereto or to the Underlying Contracts (or otherwise between the parties to such Underlying Contracts) must be clarified and settled directly with the relevant contractual partner(s), without the involvement of the Provider. This includes any disputes concerning the refunds to be paid, even where Lyfegen undertakes to claim them from a contractual partner as part of its RefaaS Services. The Customer also acknowledges and accepts that, with regard to Data-Driven Contracts (a) it will enter into the agreements necessary under the applicable Data Protection Legislation with such other contractual partner(s) to the Data-Driven Contracts and that (b) it is responsible for ensuring that such agreements comply with the applicable Data Protection Legislation. Should they be joint controllers, the Customer shall ensure that there are no conflicting instructions to the Provider and cover any costs and other consequences of the Provider related thereto.

3.2.3. In the event that the Provider provides the RefaaS Services to the Customer pursuant to a power of attorney, such provision shall be executed solely within the scope of authority granted by said power of attorney. The Provider's obligation to deliver the RefaaS Services shall be contingent upon the continuous validity and authorization conferred by the power of attorney. In the event of revocation of the relevant power of attorney by the Customer, the Provider shall cease to provide the RefaaS Services, and such cessation shall not constitute a breach of its obligations under these LTC. Notwithstanding the foregoing, a revocation of the relevant power of attorney does not affect the provisions of the SaaS Services by the Provider to the Customer under these LTC and applicable Work Order(s). If the Customer wishes to withdraw the power of attorney, it shall do so in writing vis-à-vis the Provider; upon the termination of the RefaaS Service the power of attorney shall be considered withdrawn automatically. Refund claims at all times remain claims of the Customer, and the Provider is neither entitled nor required to undertake any debt enforcement or other legal measures, unless expressly agreed otherwise with the Customer in each instance. No interest is owed by the Provider for the time during which any amounts remain on the Provider's accounts, or otherwise for the time required to forward a refund to Customer. Refund claims are at no time assigned to the Provider, and the Provider shall in no way be liable or responsible for being successful in obtaining a refund for Customer or a Contract Partner making a refund payment or otherwise complying with its obligations towards Customer, or bear the risk of such Contract Partner failing to do so (including in those cases where Provider agrees to undertake debt enforcement or other legal measures). Further, the Provider shall not be responsible for any losses due to wrong or improper account information on the power of attorney of the Customer; the Provider has no obligation to verify the correctness of such account information, and if a Contract Partner contacts the Provider for verification, it will confirm the account information contained on the power of attorney. For as long as the Customer has not withdrawn its power of attorney, and in view of the fee structure agreed, the Customer shall not interfere with or pre-empt the Provider's activities in pursuing refund claims as per the Work Order(s).

3.3. Where the Customer acts as a Supplier, as specified in the Work Order, the following applies:

3.3.1. As agreed in the relevant Work Orders, such access will cover access to the Common Modules, including access to the relevant Data-Driven Contracts and/or the Financial-Driven Contracts within the Agreements Module, and the Relevant Contract Records generated by the Agreements Module for each such Data-Driven Contract and/or Financial-Driven Contract, subject to the relevant HPPs having instructed the Provider (acting as their Processor) to make the Data-Driven Contract and/or Financial-Driven Contract and the corresponding Relevant Contract Records accessible to the Customer and having provided the necessary data, instructions and other assistance to the Provider. The Customer acknowledges and accepts that, in any event, such access will not include access to the HPP only Modules (see Work Order, e.g., the PD Mode and All-Inclusive Mode of the Data Module), so that the Customer (in its role as a Supplier) will not be granted access to the PD Mode and All-Inclusive Mode of the Data Module and its corresponding features and functionalities by the Provider as part of this Agreement, and the Provider will not provide any Data Module service in relation to the PD Mode and All-Inclusive Mode to the Customer (in its role as a Supplier) as part of this Agreement.

3.3.2. The Customer acknowledges and accepts that with regard to the Underlying Contracts, including the provision of the Relevant Contract Records to the Customer, (a) the Provider is only acting upon instruction and on behalf of the relevant HPPs using data provided to it by such HPPs, (b) the Provider is not party to the Underlying Contracts or other cooperation agreements between the parties to such Underlying Contracts, (c) any Relevant Contract Record and other data provided through the Agreements Module is provided to the Customer "as is" without any warranty whatsoever, and that it is used by the Customer at its own risk, and (d) that any issue, controversy, claim or other dispute related thereto or to the Underlying Contracts (or otherwise between the parties to such Underlying Contracts) or to specific instructions of a HPP to the Provider must be clarified and settled directly with the relevant HPPs, without the involvement of the Provider. The Customer shall cover any costs incurred by the Provider as a consequence of the Customer's failure to comply with the foregoing.

3.4. The Provider undertakes to within the Agreements Module transparently reflect to both the Customer and the Contract Partner specific digital contract algorithms and other parameters it applies for each Underlying Contract to permit both parties to the value and data-driven agreement, respectively to the value and financial-driven agreement, to validate the price of medication determined by the Agreements Module for the Underlying Contract at issue.

3.5. As agreed in the relevant Work Orders, where the Customer opted for the Sharing Module, it may share the Relevant Contract Records generated by the Agreements Module through the Lyfegen Platform to a designated Receiving Partner, as set forth in Annex 1. It is the responsibility solely of the Customer to ensure that such disclosure is permitted, that the Receiving Partner does not misuse the Relevant Contract Records or Sharing Module. The Provider will not identify or verify the identity of the designated Receiving Partner or verify that the access to the Sharing Module and the Relevant Contract Records is made by the intended Receiving Partner and not an unauthorized third-party. However, the Provider will implement technical measures that it deems appropriate to minimize the risk of unauthorized access, as may be amended by the Provider from time to time. The Provider may, for its own protection, require the Receiving Partner to accept reasonable terms prior to granting access to the Relevant Contract Records or permitting the Receiving Partner to provide a communication for Customer. The Receiving Partner is not a User and may not raise any claims against the Provider.

1. **Customer's Usage Rights**

4.1. The Provider hereby grants the Customer a non-exclusive, non-transferable, temporary limited right to access and use the Lyfegen Platform and related services for the purposes as laid out in the relevant Work Order, but in any event only for its own internal business purposes ("**Usage Right**"). The Usage Right is granted for the term of the relevant Work Order, unless suspended in accordance with this Agreement.

4.2. The Customer may exercise the Usage Rights through the Users. However, solely the Customer is entitled to claim any contractual rights or raise any claims under the Agreement.

4.3. The Customer shall not license, sell, rent, lease, transfer, assign, distribute, display, host, outsource, disclose or otherwise commercially exploit or make the Lyfegen Platform available to any third party other than a User properly authorized by the Customer.

4.4. The Customer shall not modify, make derivative works of, disassemble, reverse compile, or reverse engineer any part of the Lyfegen Platform, including without limitation the documentation that is provided as a part thereof, or access the Lyfegen Platform in order to build a similar or competitive product or service now or in the future, in any part of the world.

4.5. Except as expressly stated herein, no part of the Lyfegen Platform may be copied, reproduced, distributed, republished, downloaded, displayed, posted or transmitted in any form or by any means, including but not limited to electronic, mechanical, photocopying, recording, or other means.

4.6. The Customer agrees to make every reasonable effort to prevent unauthorized third parties from accessing or using the Lyfegen Platform.

4.7. The Customer acknowledges and agrees that the Provider or its Third Party Vendors shall own all right, title and interest in and to all intellectual property rights in the Lyfegen Platform and any suggestions, enhancement requests, feedback, or recommendations provided by the Customer or its Users relating to the Lyfegen Platform, including all unpatented inventions, patent applications, patents, design rights, copyrights, trademarks, service marks, trade names, know-how and other trade secret rights, and all other intellectual property rights, derivatives or improvements thereof.

4.8. The Customer does not acquire any rights in the Lyfegen Platform, express or implied, other than those expressly granted in this Agreement (including in the applicable Work Orders, if any), and any and all rights not expressly granted to the Customer are reserved by the Provider and Third-Party Vendor.

4.9. This Agreement is not a sale and does not convey any rights of ownership in or related to the Lyfegen Platform or products or services of Third-Party Vendors to the Customer.

1. **Use of Customer Data by Provider**

5.1. Where the Customer acts as a HPP, as specified in the Work Order, the following applies:

The Provider's Processing and right to use Customer Data for its own purposes (and as a Controller, insofar it contains Personal Data) is set forth in Annex 4. It is the responsibility of the Customer to ensure that such usage is compliant with its agreements with relevant Contract Partners.

1. **Intellectual Property Rights**

6.1. The Lyfegen Platform and any necessary software used in connection with it contains proprietary and confidential information that is protected by applicable intellectual property and other Laws. Further, the content or information presented to the Customer through the Lyfegen Platform may be protected by copyrights, trademarks, service marks, patents or other proprietary rights and Laws. Except where expressly provided otherwise by the Provider, nothing in the Lyfegen Platform or this Agreement shall be construed to confer any license to any of the Provider's or its third party manufacturer's, author's, developer's, vendor's, and service provider's ("**Third-Party Vendors**"), intellectual property rights.

1. **Terms of Service**

7.1. Any new feature that augments or enhances the Lyfegen Platform, and/or any new Data-Driven Contract, Financial-Driven Contract or service subsequently purchased or subscribed to by the Customer will be subject to this Agreement.

7.2. The Customer may designate Users and allow them access to the Lyfegen Platform. For such purpose, the Customer or the Provider on the Customer's behalf will provide and assign unique password and usernames to each authorized User, or otherwise grant such Users access rights to the Lyfegen Platform. The Customer acknowledges and agrees that it is prohibited from sharing passwords and usernames with unauthorized users. The Customer will be solely responsible for the confidentiality and use of the Customer's (including its employees') passwords and usernames as well as for the management of access rights of Users.

7.3. The Provider will make commercially reasonable efforts to support the Customer's successful utilization of the Lyfegen Platform as intended by the Parties, including but not limited to maintenance and support of the Lyfegen Platform as provided in Annex 3, providing the Customer with user guides, on-line help and product support. The Provider also offers "for fee" extended support options and professional services consultation, which services may include, among other things, training services, business and regulatory process consulting, and system configuration. Additionally, the Provider will make commercially reasonable efforts to ensure it maintains the system availability of the Lyfegen SaaS Services as set forth in Annex 3.

7.4. The Provider may fully or partially subcontract or otherwise use third parties in connection with its performance of this Agreement to third parties inside and outside of the country of the Provider's domicile, it being understood that the Provider remains responsible for the proper performance of this Agreement. In particular, the Provider may use carefully selected cloud service providers for hosting the Lyfegen Platform (including, e.g., Amazon Web Services, Google or Microsoft; the specific subprocessors used are listed in Annex 5A), with the Customer agreeing and accepting that the Provider's obligations and liability under this Agreement with regard to such subcontracting shall be subject to their obligations and liability towards the Provider under their standard terms and conditions. The Customer acknowledges and agrees to the commissioning of the subcontractors (which may also be sub-processors, as the case may be) listed in Annex 5A to this Agreement (including as per the special terms in Annex 5A).

1. **Customer's Responsibilities**

8.1. The Customer is responsible for all activities that occur under the Customer's use of the Lyfegen Platform (including the User's access credentials), regardless of whether the activities are authorized or undertaken by the Customer, its Users or a third party. The Provider is not responsible for unauthorized access to the Lyfegen Platform using accounts of Users or otherwise using access of credentials, e-mails or other resources or identification of the Customer, except to the extent caused by the Provider's breach of this Agreement.

8.2. The Customer shall comply with all Laws applicable to the Customer in connection with its use of the Lyfegen Platform or use or consumption of the Provider's other services, including without limitation Data Protection Legislation, and Laws related to handling of health data, international communications, and the exportation of technical data.

8.3. The Customer agrees to notify the Provider immediately of any unauthorized use of any password or account or any other known or suspected breach of security or any known or suspected distribution of Customer Data.

8.4. Any action performed on the Lyfegen Platform by a User shall be deemed an action of the Customer and authorized by the Customer. The Customer shall be responsible for the conduct of its Users as for its own conduct. As part of the foregoing, the Customer agrees that any Administrator may, with binding effect for the Customer, agree to the activation or deactivation of features and functions, or change in configuration, of the Lyfegen Platform and related SaaS Services, and changes of these LTC. Such agreement may be given through an online process implemented on the Lyfegen Platform ("click-wrap" or through configuration or service settings).

1. **Suspension**

9.1. The Customer agrees that the Provider may, with reasonably contemporaneous telephonic or electronic mail notice to the Customer, suspend the Customer's access to the Lyfegen Platform or other provision of services if the Provider reasonably concludes that the Customer's use of the Lyfegen Platform or a third-party activity (e.g., a cyber-attack) is causing immediate and ongoing harm to the Provider, the Lyfegen Platform or others.

9.2. The Provider will use commercially reasonable efforts to resolve the issues causing the suspension. The Customer agrees that the Provider will not be liable to the Customer or to any third party for any suspension of the Lyfegen Platform under such circumstances as described in this Section.

1. **Modification or Discontinuation**

10.1. The Provider reserves the right at any time and from time to time to modify, temporarily or permanently, the Lyfegen Platform (or any part thereof) or other services.

10.2. Notwithstanding the foregoing, except for routinely scheduled down time, or as otherwise provided in this Agreement, the Provider shall use commercially reasonable efforts to notify the Customer prior to any such modification.

10.3. The Customer acknowledges that the Provider reserves the right to discontinue offering the Lyfegen Platform or any other services at any time. The Customer agrees that the Provider will not be liable to the Customer or any third party for any modification or discontinuance of the Lyfegen Platform or other services as described in this Section 10.

10.4. The aforementioned rights shall include the right of the Provider to, without liability, amend Annex 1 from time to time, with such amendments being announced at least 60 days before taking effect. In case of material changes to the detriment of the Customer, the Customer may extraordinarily terminate the affected Work Orders without liability by giving notice within the 30 days following to notification of the change. Such amendments may also include the addition and the removal of features and functionalities of the Lyfegen Platform or other services. The Provider will undertake to keep the Customer informed of its plans to develop the Lyfegen Platform, but such information shall be provided on an informational basis only without binding effect. The Customer also understands and accepts that the Lyfegen Platform is a standardized solution not specifically designed for the Customer, and may not provide for, or maintain, all features and functionalities the Customer may need in its particular situation, and any representation, warranty and undertaking related thereto is hereby disclaimed by the Provider.

1. **Confidentiality**

11.1. Each Party may have access to information that is confidential to the other Party ("Confidential Information"). For the purposes of this Agreement, Confidential Information shall include any information that is clearly identified in writing at the time of disclosure as confidential as well as any information that, based on the circumstances under which it was disclosed, a reasonable person would believe to be confidential.

11.2. Notwithstanding the foregoing, a Party's Confidential Information shall not include information that (i) is or becomes a part of the public domain through no act or omission of the other Party; (ii) was in the other Party's lawful possession prior to the disclosure without any obligation of confidentiality and had not been obtained by the other Party either directly or indirectly from the disclosing Party; (iii) is lawfully disclosed to the other Party by a third party without restriction on disclosure; (iv) is independently developed by the other Party without use of or reference to the other Party's Confidential Information, as established by written records.

11.3. The Parties undertake to maintain strict confidence with respect to all Confidential Information of the other Party and to use commercially reasonable efforts not to make each other's Confidential Information available in any form to any third party in whole or in part outside the scope of the products and services as set forth in the Agreement. Notwithstanding the foregoing, the Customer acknowledges and agrees that the Provider may disclose the Customer's Confidential Information (a) to its Third Party Vendors solely to the extent necessary to provide products or services under this Agreement, and (b) as otherwise set forth by this Agreement, in particular as set forth in Section 5.

11.4. This Section will not be construed to prohibit disclosure of Confidential Information to the extent that such disclosure is required by Law or valid order of a court or other governmental authority; provided, however, that a Party who has been subpoenaed or otherwise compelled by a valid Law or court order to disclose Confidential Information (the "**Responding Party**") shall first have given sufficient and prompt written notice to the other Party of the receipt of any subpoena or other request for such disclosure, so as to permit such Party an opportunity to obtain a protective order or take other appropriate action. The Responding Party will cooperate in the other Party's efforts to obtain a protective order or other reasonable assurance that confidential treatment will be afforded the Confidential Information. If the Responding Party is compelled as a matter of law to disclose the Confidential Information, it may disclose to the party compelling the disclosure only that part of the Confidential Information as is required by Law to be disclosed.

11.5. This Section shall also not be construed to prohibit the usage and disclosure of any work results or know-how gained by the Provider in the performance of this Agreement, it being understood that neither shall the Customer be identifiable to third parties not bound by confidentiality in connection with any such usage or disclosure, nor shall such usage or disclosure involve Personal Data of Customer.

11.6. For the avoidance of doubt, this Section shall not apply where the Provider shares the Relevant Contract Record of a particular Underlying Contract, the Underlying Contract and information required to understand and validate such Underlying Contract or Relevant Contract Record, with the other party to the value-based agreement of the Customer to which such Underlying Contract relates. Such sharing is an essential part of the Lyfegen Platform and permitted.

1. **Data Protection and Data Regulations**

12.1. Where the Customer acts as a HPP, as specified in the Work Order, the following applies:

12.1.1. With regard to the Processing of Personal Data under this Agreement, Annex 4 sets forth the Parties' understanding with regard to their respective roles as Controllers and Processors of Personal Data to be Processed under this Agreement. Further, insofar as the Processing of Customer Data is subject to clinical data regulations, professional secrecy and any other Laws and regulations (except for Laws and regulations applying to providers of SaaS in general), including any other local Laws and regulations to which the Customer is subject ("**Other Applicable Laws**"), the Customer shall be responsible that the Processing of Customer Data under this Agreement and the use of the Lyfegen Platform as provided for by the Agreement, including the instructions given to the Provider, are and remain in compliance with the Other Applicable Laws, without the Provider having any duty to verify such compliance or reason to believe that the Processing of Customer Data under this Agreement and the use of the Lyfegen Platform as provided for by this Agreement do not comply with the Other Applicable Laws. Should the Customer find out or have reason to believe that the Processing of Customer Data under this Agreement and the use of the Lyfegen Platform as provided for by this Agreement are not in compliance with the Other Applicable Laws, including without limitation following a change in the Other Applicable Laws, it shall promptly notify the Provider. Following such notification, the Parties shall promptly determine the appropriate measures to be taken in the given circumstances in order to remedy such non-compliance. The Customer shall also be responsible vis-à-vis the Provider for the use of Data-Driven Contract Records and other Personal Data of healthcare providers, payers and suppliers of medication with which the Customer has concluded Data-Driven Contracts and to which such information is provided by the Provider as per its instruction under this Agreement.

12.1.2. Where the Customer acts as a Controller with regard to the Processing of Personal Data under this Agreement, in particular with regard to Processing of Customer Data and Data-Driven Contract Records to the extent they contain Personal Data, the Customer shall comply with any and all Data Protection Legislation applicable to it with regard to the Processing of such Personal Data under or in connection with this Agreement, including responding to any Data Subject request (the Customer understands that its use of the Lyfegen Platform and compliance with any terms hereunder shall not be considered as proof or indication of compliance with any Data Protection Legislation). It is the obligation of the Customer to ensure that such use is compliant. With regard to the Data-Driven Contract Records, the Customer warrants to the Provider that all Users and other persons who have access to or otherwise receive the Data-Driven Contract Records, including any Personal Data contained therein, are alternatively (a) located in a country that provides an adequate level of data protection under Data Protection Legislation (b) located in the country where the Personal Data was originally collected from the Data Subjects or (c) otherwise contractually bound by obligations that guarantee adequate data protection.

12.1.3. The Customer shall be responsible for any Customer Data uploaded into or otherwise provided to the Data Module and, thus, to the Provider for the Provider's Processing under this Agreement. The Customer may do so only if and to the extent that it has ensured under applicable Data Protection Legislation and Other Applicable Laws (including regulating secondary use of clinical data and professional secrecy) that any such Customer Data, including any Personal Data contained therein, may lawfully be Processed as foreseen under this Agreement, including in particular for the purposes and as set forth in Annex 4. In particular, the Customer is responsible for any notices, consents (and the consequences of the revocation of such consent by a Data Subject, including any costs resulting therefrom in the case that such revocation requires the Provider to amend its Processing under this Agreement), authorizations (e.g., from regulators, supervisory authorities, ethics committees) and legal grounds required under applicable Data Protection Legislation and Other Applicable Laws. As part of the foregoing, the Customer shall inform any affected Data Subjects that (i) their Personal Data may be transferred to and Processed by the Provider for the purposes of the Agreement, (ii) that the Provider may process their Personal Data as a Controller as set forth in Annex 4 (the Customer shall in particular point Data Subjects to the data protection statement of the Provider), and (iii) that the Data-Driven Contract Records generated by Agreements Module to the extent they contain Personal Data, may be shared with the healthcare providers, payers and suppliers of medication with which the Customer has concluded Data-Driven Contracts or are involved in the performance of such Data-Driven Contracts and with the other recipients provided for by the Agreement, including Receiving Partners designated by the Customer in relation to the Sharing Module. The Customer shall enter into with each such other party any arrangement required under the applicable Data Protection Legislation, in particular where the Customer and such other party are joint Controllers. In the event that the Customer is a joint Controller with such other party, the Customer shall be, and shall procure that it is, the "lead" Controller and single point of contact for the Provider, unless agreed otherwise in the relevant Work Order. The Customer agrees to indemnify and hold harmless the Provider in case of any losses, costs, expenses and third-party claims incurred by the Provider as a result of the Customer's failure to comply with the Sections 12.1.1–12.1.3, including as a result of the Customer's use of the Data-Driven Contract Records and other Personal Data of healthcare providers, payers and suppliers of medication for purposes that are incompatible with the present Agreement and/or Other Applicable Laws and Data Protection Legislation.

12.1.4. Where the Provider acts as a Processor of the Customer with regard to the Processing of Personal Data, such as Customer Data and Data-Driven Contract Records to the extent they contain Personal Data, the Processing is further specified in Annex 4 and the Lyfegen Platform Data Processing Addendum in Annex 5 shall apply to such Processing of Personal Data by the Provider, unless agreed otherwise in the applicable Work Order. The Provider understands and accepts that Customer Data may be subject to professional secrecy as per applicable Laws, and agrees to protect it accordingly as set out in the Agreement. If the Customer requires, the Provider's own staff with access to Customer Data of patients in clear-text shall sign an adequate confidentiality declaration. The right to instruct the Provider in Processing such Customer Data for and on behalf of the Customer is regulated in Annex 5. The Customer agrees to cover the costs and other consequences as a result of the Customer providing new or different instructions than the instructions already agreed herein or from support requested by the Customer from the Provider in connection with compliance with Data Protection Legislation or Other Applicable Laws applicable to Customer.

12.1.5. Where the Provider acts as a Controller with regard to the Processing of Personal Data under this Agreement, such as the Processing of Personal Data of Users for the operation of the Lyfegen Platform or certain ancillary services, the Provider shall follow applicable Data Protection Legislation within its organization of the Provider and the systems operated by it. The Customer shall provide the Provider any reasonably requested assistance in doing so, in particular in connection with responding to, and complying with, requests or complaints from Users and other Data Subjects within Customer's domains. The Provider shall not process Personal Data provided by the Customer other than as set forth in Annex 4 (or otherwise agreed in the applicable Work Order) or permitted or required by applicable Law.

12.2. Where the Customer acts as a Supplier, as specified in the Work Order, the following applies:
12.2.1. The Customer acknowledges and accepts that with regard to any Personal Data contained in the Data-Driven Contract Records and any other information made available to the Customer through the Agreements Module, the Provider is acting as the Processor of the HPP with which the Customer has entered into the relevant the Data-Driven Contract (see Section 3.3.2). The Customer shall enter into with each such HPP any arrangement required under the applicable Data Protection Legislation, in particular where the Customer and the HPP are joint Controllers. In the event that the Customer is a joint Controller with the HPP of a particular Data-Driven Contract, the HPP shall be the "lead" Controller and single point of contact for the Provider, and the Customer shall act vis-à-vis the Provider only through the lead Controller to the extent permitted by applicable Law, unless agreed otherwise in the relevant Work Order. Any costs incurred by the Provider due to any acts or omissions of the Customer as a joint Controller, or non-compliance with the foregoing, shall be borne by the Customer.

12.2.2. The Customer understands and accepts that the Data-Driven Contract Records and any other information obtained through the Agreements Module under this Agreement may contain Personal Data. The Customer warrants to the Provider that all Users and other persons who have access to or otherwise receive the Data-Driven Contract Records, including any Personal Data contained therein, are alternatively (a) located in a country that provides an adequate level of data protection under Data Protection Legislation (b) located in the country where the Personal Data was originally collected from the Data Subjects or (c) otherwise contractually bound by obligations that guarantee adequate data protection. The Customer shall use any such Data-Driven Contract Records and other Customer Data solely for the purposes of the relevant Data-Driven Contract it has entered into with the relevant HPP and as provided for by the Work Order, which purposes shall be compatible with applicable Law, unless the HPP has authorized the Customer otherwise. In particular, the Customer shall not to use such Data-Driven Contract Records and other Customer Data provided to it through the Agreements Module for human research or other regulated activities under applicable Law, unless the HPP has authorized the Customer otherwise. In the latter case, such authorization shall be obtained directly from the HPP by the Customer and the Customer agrees to hold the Provider harmless against any consequences resulting from any such arrangement between the HPP and the Customer, which shall be binding only on the HPP and the Customer. In any event, the sole responsibility for the Customer's Processing and other use of Data-Driven Contract Records and any other Customer Data shall be with the Customer, and not the Provider. The Customer shall comply with any applicable Laws and regulations, including any applicable Data Protection Legislation, when Processing and otherwise using Data-Driven Contract Records and any other Customer Data, and the Customer shall indemnify and hold harmless the Provider against any costs, damages and claims as a consequence of the Customer's alleged or actual non-compliance with its obligations as per this Section 12.2 (the Customer understands that its use of the Lyfegen Platform and compliance with any terms hereunder shall not be considered as proof or indication of compliance with any Data Protection Legislation).

12.2.3. Where the Provider acts as a Processor of the Customer with regard to the Processing of Customer Data, the Processing shall be further specified in the Work Order and the Lyfegen Platform Data Processing Addendum in Annex 5 shall apply to such Processing of Personal Data by the Provider, unless agreed otherwise in the applicable Work Order. The right to instruct the Provider in Processing such Customer Data for and on behalf of the Customer is regulated in Annex 5. The Customer agrees to cover the costs and other consequences as a result of the Customer providing new or different instructions than the instructions already agreed herein or from support requested by the Customer from the Provider in connection with compliance with Data Protection Legislation or other Laws applicable to the Customer.

12.2.4. Where the Provider acts as a Controller with regard to the Processing of Personal Data under this Agreement, such as the Processing of Personal Data of Users for the operation of the Lyfegen Platform or certain ancillary services, the Provider shall follow applicable Data Protection Legislation within its organization and the systems operated by it. The Customer shall provide the Provider any reasonably requested assistance in doing so, in particular in connection with responding to, and complying with, requests or complaints from Users and other Data Subjects within the Customer's domain. The Provider shall not process Personal Data provided by the Customer other than as set forth in this Agreement or as permitted or required by applicable Law. With regard to its Users, the Customer shall have them informed about the Processing of their Personal Data by the Provider (including by pointing them to the Provider's data protection statement), and shall ensure that their Personal Data is lawfully transferred into the Provider's domain and may be Processed by the Provider as set forth herein. The same shall apply *mutatis mutandis* to any Personal Data the Customer may provide to the Provider under this Agreement.

12.3. With regard to the Data-Driven Contract Records, either Party may request from time to time to enter into an additional agreement with the other Party to govern the transfer of the Data-Driven Contract Records to the Customer, including the EU Processor-to-Controller clauses released by the European Commission from time to time, and the other Party shall accept to enter into such an agreement.

12.4. In addition to the Sections 12.1 and 12.2, as applicable, if HIPAA/HITECH is applicable, as specified in the Work Order, the following additionally apply: With respect to Personal Data which is protected health information, as such term is defined in HIPAA and HITECH, the Parties agree to be bound by the terms of the Business Associate Agreement set forth in Annex 6.

1. **Data Security**

13.1. The Provider shall maintain a formal security program materially in accordance with industry standards that is designed to: (i) ensure the security and integrity of Customer Data; (ii) protect against threats or hazards to the security or integrity of Customer Data; and (iii) prevent unauthorized access to Customer Data, all of the foregoing being subject to the provisions of Annex 5.

13.2. The current security measures of the Provider are outlined in Annex 2 attached hereto, which may be amended from time to time by the Provider. With regard to cloud hosting providers used by the Provider, their own set of data security measures shall apply.

1. **DISCLAIMER OF WARRANTIES**

14.1. THE PROVIDER DOES NOT REPRESENT THAT THE CUSTOMER'S USE OF THE LYFEGEN PLATFORM (INCLUDING ANY DATA AND OTHER CONTENT CONTAINED THEREIN OR PROCESSED THEREBY) WILL BE SECURE, TIMELY, UNINTERRUPED OR ERROR FREE, OR THAT THE LYFEGEN PLATFORM WILL MEET THE CUSTOMER REQUIREMENTS OR THAT ALL ERRORS IN THE LYFEGEN PLATFORM, ITS DATA/CONTENT AND/OR DOCUMENTATION WILL BE CORRECTED OR THAT THE SYSTEM THAT MAKES THE LYFEGEN PLATFORM AVAILABLE WILL BE FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS OR THE LYFEGEN PLATFORM WILL OPERATE IN COMBINATION WITH OTHER HARDWARE, SOFTWARE, SYSTEMS OR DATA NOT PROVIDED BY THE PROVIDER OR THE OPERATION OF THE LYFEGEN PLATFORM WILL BE SECURE OR THAT THE PROVIDER AND ITS THIRD PARTY VENDORS WILL BE ABLE TO PREVENT THIRD PARTIES FROM ACCESSING CUSTOMER DATA OR THE CUSTOMER'S

CONFIDENTIAL INFORMATION, OR ANY ERRORS WILL BE CORRECTED OR ANY STORED OR OTHERWISE PROCESSED CUSTOMER DATA WILL BE ACCURATE, TIMELY, COMPLETE OR RELIABLE.

14.2. THERE ARE NO WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, THOSE OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THE LYFEGEN PLATFORM IS PROVIDED TO THE CUSTOMER ON AN "AS IS" AND "AS AVAILABLE" BASIS AND IS FOR COMMERCIAL USE ONLY. THE CUSTOMER ASSUMES ALL RESPONSIBILITY FOR DETERMINING WHETHER THE LYFEGEN PLATFORM OR THE INFORMATION GENERATED THEREBY IS ACCURATE OR SUFFICIENT FOR THE CUSTOMER'S PURPOSE.

1. **LIMITATIONS OF LIABILITY**

15.1. NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY FOR EXEMPLARY, PUNITIVE, SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES INCLUDING WITHOUT LIMITATION, INTERRUPTION OF BUSINESS, LOST PROFITS, LOST OR CORRUPTED DATA OR CONTENT, LOST REVENUE ARISING OUT OF THIS AGREEMENT (INCLUDING THE WORK ORDERS) (INCLUDING WITHOUT LIMITATION THE LYFEGEN PLATFORM, THE USE OF THE LYFEGEN PLATFORM OR THE INABILITY TO USE THE LYFEGEN PLATFORM), EVEN IF THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

15.2. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF THE PROVIDER OR ANY THIRD PARTY VENDORS ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT (INCLUDING THE WORK ORDERS), INCLUDING ANY LICENSE, USE, OR OTHER EMPLOYMENT OF THE LYFEGEN PLATFORM, WHETHER SUCH LIABILITY ARISES FROM ANY CLAIM BASED ON BREACH OR REPUDIATION OF CONTRACT, BREACH OF WARRANTY, TORT, OR OTHERWISE, EXCEED THE TOTAL AMOUNTS ACTUALLY PAID BY THE CUSTOMER IN THE SIX (6) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO SUCH CLAIM (IF ANY). THERE SHALL BE ONLY ONE AGGREGATE LIABILITY CAP UNDER THIS AGREEMENT EVEN IF THERE ARE MULTIPLE CLAIMS; EACH CLAIM SHALL REDUCE THE AMOUNT AVAILABLE IN THE AGGREGATE LIABILITY CAP.

15.3. THE PROVIDER SHALL NOT BE LIABLE FOR ANY DAMAGES RESULTING FROM THE LOSS OR CORRUPTION OF ANY DATA OR CONTENT WHETHER RESULTING FROM DELAYS, NONDELIVERIES, MISDELIVERIES, SERVICE INTERRUPTIONS OR OTHERWISE.

15.4. THE EXCLUSIONS AND LIMITATIONS OF LIABILITY SET FORTH IN THIS SECTION SHALL NOT APPLY WITH RESPECT TO:
15.4.1. DAMAGES TO PERSONS AND/OR TANGIBLE PROPERTY OCCASIONED BY THE WILLFUL MISCONDUCT OR GROSS NEGLIGENCE OF A PARTY,
15.4.2. BREACHES BY THE CUSTOMER OF LICENSE TERMS APPLICABLE TO SOFTWARE PROVIDED BY THE PROVIDER,
15.4.3. THE CUSTOMER'S UNAUTHORIZED USE OF THE PROVIDER'S OR THIRD-PARTY VENDOR'S INTELLECTUAL PROPERTY, MATERIALS OR ASSETS;
15.4.4. DAMAGES AS LIMITED BY THIS SECTION 15 ARE THE CUSTOMER'S SOLE AND EXCLUSIVE REMEDY IF ANOTHER REMEDY IS PROVIDED AND SUCH REMEDY IS DEEMED TO FAIL OF ITS ESSENTIAL PURPOSE.

1. **Customer's Indemnity**

16.1. The Customer shall defend and indemnify the Provider and its Third Party Vendors against any and all Losses incurred by the Provider and its Third Party Vendors arising out of or in connection with a claim by a third party (i) alleging that the Customer Data or the Customer Trademarks, or any use thereof, infringes the rights of, or has caused harm to, a third party, or (ii) arising out of the Customer's breach of Section 8.

16.2. The Customer will indemnify, defend and hold harmless the Provider, its affiliates, successors, and assigns, including the applicable officers, directors, employees, and agents thereof for damages, costs and attorneys' fees the Provider incurs from any unaffiliated third-party claim arising from the Customer's or any User's use of the Lyfegen Platform.

1. **Fees and Payment Terms**

17.1. Setup and implementation costs are to be paid as agreed in the applicable Work Order and/or when ordered during the Agreement. The fees for the Lyfegen Platform are invoiced as agreed in the applicable Work Order. The Customer shall pay the respective invoices within thirty (30) days after receipt thereof, without any deductions.

17.2. In addition to any remedies the Provider may have pursuant to this Agreement or at Law for non-payment, delinquency in payment shall entitle the Provider to delay or suspend the right of the Customer and restrict the ability to use the Lyfegen Platform, in total or in part.

17.3. In the event the Provider incurs any costs (including reasonable attorney's fees) from efforts collecting overdue fees from the Customer, the Customer agrees to pay such costs. The Customer further agrees to pay all foreign, federal, states, and local taxes, if applicable, to Customer's access to, use, or receipt of the Lyfegen Platform.

17.4. In the case of a RefaaS Service, where agreed in the Work Order, the Provider may obtain from the Customer the agreed fees for providing such services by deducting the relevant amounts (and VAT) from any amounts received on its accounts. It shall provide the Customer with a balance statement detailing such deduction. In all other cases, the Customer shall pay the fees upon invoice within thirty (30) days after the receipt thereof, without any deductions. The Customer agrees that it owes to the Provider, and shall pay, the fees for the RefaaS Service applicable to any refunds that are received by the Customer and are or have been subject to a RefaaS Service as per a valid Work Order regardless of whether such refunds are paid to the Customer (i) directly, through the Provider or a third-party, (ii) due to acts or omissions of the Provider, the Customer or a third-party and (iii) during the term of Work Order or thereafter.

1. **Term and Termination**

18.1. This Agreement will commence on the Start Date of the Work Order. In the event that the Parties conclude several Work Orders, this Agreement will commence on the Start Date of the first Work Order for the term provided in each such Work Order.

18.2. Each Party may terminate a Work Order upon one hundred and eighty (180) days' written notice to the other Party, subject, however, to any minimum term set forth by a Work Order (in which case the Work Order may not be terminated before the minimum term has expired).

18.3. The termination or expiration of a Work Order shall not affect the validity of any remaining Work Order. If upon termination of one or several Work Orders, no Work Order would remain, the Agreement shall terminate upon the term of the last existing Work Order.

18.4. The Provider may terminate any Work Order or suspend the performance of a Work Order without prior notice and without liability if it reasonably concludes that the Underlying Contract or the contract of the Provider with the Contract Partner is not complied with.

18.5. The right of each Party to terminate a Work Order extraordinarily for "important reasons" shall remain reserved. The material breach of this Agreement shall be considered an important reason, provided that if such breach can be remedied, the Party in breach shall be given a grace period of at least thirty (30) days to remedy such breach before the Agreement or Work Order may be terminated. The non-compliance with the restrictions to use the Lyfegen Platform and the non-payment of the Fees shall be considered a material breach.

18.6. Upon the termination of a Work Order, the Provider shall provide the Customer with a copy of Customer Data, including the Data-Driven Contract Records, and Pricing Data, including the Financial-Driven Contract Records, in an electronic form, with such work being chargeable at the Provider's standard rates. Any other termination support shall be mutually agreed by the Parties. The termination of a Work Order shall not be interpreted as a termination of the Data-Driven Contracts and the Financial-Driven Contracts to which the Customer may be subscribed. However, it will be the Customer's responsibility to provide for the necessary measures to be able to continue with such Data-Driven Contracts and Financial-Driven Contracts. Once the Provider has provided the Customer with a copy of the Customer Data, including the Data-Driven Contracts Records, and the Pricing Data, including the Financial-Driven Contract Records, the Provider shall have no obligation to retain any Customer Data, Pricing Datat, or other data related to the Customer. The Customer acknowledges and accepts that the termination of a Work Order may make it impossible to further comply with value-based agreements it may have with other contractual partners.

1. **Notices**

19.1. If not provided otherwise in the Agreement, any notice required or permitted under the terms of the Agreement or required by Law must be in writing and must be (a) delivered in person, (b) sent by registered or certified mail return receipt requested, (c) sent by overnight courier, (d) sent by facsimile (with a hard copy mailed on the same date), or (e) sent by email whose receipt is acknowledged by an officer of the receiving Party.

1. **Amendment**

20.1. Save as provided for below, changes to this Agreement (including its Work Orders) are valid only if agreed to in writing by the Parties, including by use of electronic signing services such as DocuSign and Adobe Sign, or by use of an online process implemented in the Lyfegen Platform. Each Administrator shall be considered authorized to fully represent, and act for, the Customer with regard to such changes or the conclusion of further Work Orders under this Agreement.

20.2. The Provider may unilaterally modify or amend these LTC (including their annexes) at any time. The proposed amendments will be notified to the Customer at least thirty (30) days prior to the proposed effective date of the amendment in text form (including e-mail). Unless within ten (10) days of the date of the notification Customer so notified delivers to Provider a written notice containing a reasoned objection against the proposed amendment to the LTC, the amendment shall be deemed accepted by Customer.

20.3. If the Customer does not timely object to a proposed amendment, then the amendment shall become effective and the LTC as amended shall apply between the Parties and to all ongoing Work Orders and replace the previous version of the LTC. If the Customer timely objects to an amendment, then the LTC prior to the amendment shall continue to apply unchanged between the Parties, however with the Provider having the right to terminate the Agreement in part or total without liability with a thirty (30) day written notice, provided the amendment of the LTC was proposed for good cause.

1. **Survival**

21.1. The following provisions of this Agreement shall in any event survive any completion, rescission, expiration or termination of this Agreement: Sections 3.2.2 and 3.3.2 (Provision of Services), 5 (Use of Customer Data by Provider), 6. (Intellectual Property Rights), 11. (Confidentiality) 14. (DISCLAIMER OF WARRANTIES), 15. (LIMITATIONS OF LIABILITY), 16. (Customer's Indemnity).

1. **Assignment**

22.1. Neither Party may assign any of its rights or obligations under this Agreement, whether by operation of law or otherwise, without the prior written consent of the other Party (which consent shall not be unreasonably withheld). Notwithstanding anything herein to the contrary, Lyfegen shall be permitted to assign rights and obligations under this Agreement to an affiliated or subsidiary company, including Lyfegen HealthTech AG (where the latter is not itself the Provider).

22.2. Notwithstanding the foregoing, either Party may assign this Agreement in its entirety without consent of the other Party in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets provided the assignee has agreed to be bound by all of the terms of this Agreement and all past due fees are paid in full, except that the Customer shall have no right to assign this Agreement to a direct competitor of the Provider.

22.3. Any attempt by a Party to assign its rights or obligations under this Agreement in breach of this Section shall be void and of no effect.

22.4. Subject to the foregoing, this Agreement shall bind and inure to the benefit of the Parties, their respective successors and permitted assigns.

1. **Force Majeure**

23.1. Neither Party will be liable to the other for any failure or delay in the performance of such Party's non-monetary obligations due to causes beyond its control, such as failure or delay caused, directly or indirectly, by fire, flood, earthquakes, other elements of nature, acts of war, terrorism, riots, civil disorders, rebellions or revolutions, epidemics, communications line or power failures, or governmental Laws, court orders, and regulations imposed after the fact.

1. **Marketing**

24.1. The Customer shall grant the Provider permission to use the Customer's name and logo in its or its Affiliate's marketing materials and website for the purpose of indicating a commercial relationship between the Customer and the Provider. Furthermore, the Customer shall support the conduct of a case study providing feedback and testimonials upon request of the Provider.

24.2. The Customer shall agree to a press release where the Provider announces that the Customer is joining the Lyfegen Platform.

1. **Relationship of the Parties**

25.1. The Parties are independent contractors. This Agreement does not create nor is it intended to create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the Parties. There are no third-party beneficiaries to this Agreement.

1. **Final Provisions**

26.1. At no time shall any failure or delay by either Party in enforcing any provisions, exercising any option, or requiring performance of any provisions, be construed to be a waiver of the same.

26.2. If any provision of this Agreement is for any reason held to be invalid, illegal or unenforceable under applicable Law, the remaining provisions of the same shall be unimpaired, and the invalid, illegal or unenforceable provision shall be replaced by a valid, legal and enforceable provision that comes closest to the intention of the Parties underlying the original provision.

1. **Dispute Resolution**

27.1. Prior to initiation of any court procedure, the Parties shall endeavour to settle amicably by direct informal negotiation any disagreement or dispute arising out of or in connection with this Agreement.

1. **Applicable Law and Place of Jurisdiction**

28.1. This Agreement, and all the rights and duties of the Parties arising out of or in connection with this Agreement, is governed, construed and enforced by the substantive Laws according the following table:

Domicile of Provider	**Applicable Law**
Switzerland	Laws of Switzerland whereby (i) international conventions, including the United Nations Convention on Contracts for the International Sale of Goods of 11.04.1980 (CISG) and (ii) Swiss conflict of law rules are hereby excluded from application to this Agreement.
USA	Laws of Delaware

28.2. The courts according the following table shall have exclusive jurisdiction with regards to any dispute arising between the Parties out of or in connection with this Agreement (including its interpretation, closing, execution, binding effect, amendment, breach, termination or enforcement).

Domicile of Provider	Applicable Law
Switzerland	The ordinary courts of the City of Basel, Switzerland
USA	The federal and state courts of the Wilmington, Delaware, USA

ANNEX 1: FUNCTIONAL DESCRIPTION OF THE LYFEGEN PLATFORM AND ITS ANCILLARY SERVICES

SaaS Services

COMMON MODULES

1. AGREEMENTS MODULE

The Agreements Module is a SaaS service provided using a cloud-based application that allows the programming, management and monitoring of Data-Driven Contract(s) or Financial-Driven Contract(s), or both, as the case may be. It includes access to the Data-Driven Contract Records and Financial-Driven Contract Records and other Data-Driven Contract data by both the Customer and the Contract Partner of those patients and their treatments and events that are covered by the Data-Driven Contract and/or Financial-Driven Contract.

2. FINANCIALS MODULE

The Financials Module is a SaaS service provided using a cloud-based application that allows initiating potential premium payments or potential refunds, as the case may be.

3. CASES MODULE

The Cases Module, for mapping all reimbursement-relevant cases at the patient level. Patients are tracked, including a listing of all associated reimbursements, from the issuance of the cost authorization to the completion of therapy.

SUPPLIER ONLY MODULES

4. Data Module (NPD MODE)

The Data Module is a SaaS service provided using a cloud-based application that, in the NPD Mode, allows to register and manage Pricing Data, including financial data records of a particular medication, with such Pricing Data being Processed by the Agreements Module in connection with Financial-Driven Contract(s).

HPP ONLY MODULES

5. DATA MODULE (PD MODE)

The Data Module is a SaaS service provided using a cloud-based application that, in the PD Mode, allows to register and manage Customer Data, including event data records related to the treatment of individual patients, with such Customer Data being Processed by the Agreements Module in connection with Data-Driven Contract(s).

6. Data Module (ALL INCLUSIVE MODE)

The Data Module is a SaaS service provided using a Cloud-based application that, in the All-Inclusive Mode, allows to register and manage (a) Customer Data, including event data records related to the treatment of individual patients, with such Customer Data being Processed by the Agreements Module in connection with Data-Driven Contract(s) as per the PD Mode and (b) Pricing Data, including financial data records of a particular medication, with such Pricing Data being Processed by the Agreements Module in connection with Financial-Driven Contract(s).

7. SHARING Module

The Sharing Module is a SaaS service provided using a cloud-based application that enables the Customer to share a Relevant Contract Record with a designated Receiving Partner it (e.g., by way of a download link, limited in time) and communicate with that Receiving Partner through the Lyfegen Platform. The Receiving Partner is not necessarily a contract party to the Provider.

REFAAS Services

The RefaaS Services are ancillary services provided by the Provider in addition to its main SaaS Services under these LTC, whereby the Provider handles and processes the Customer's by default all – or, if agreed differently in the relevant Work Order(s), the agreed – refund cases against its Contract Partner(s) (acting as Supplier) in connection with all of Customer's Data-Driven and/or Financial-Driven Contracts implemented in the Agreements Module for and on behalf of the Customer (acting under a power of attorney to be provider by Customer), always provided (i) the claim related to a particular refund case has become due during the term of the RefaaS Service, (ii) and the Provider has not opt-out from handling and processing such refund case (which the Provider may do at its discretion by providing notice to the Customer). The relevant contracts (i.e. Data-Driven Contract[s], Financial-Driven Contract[s], or both) are implemented in the Agreements Module and fed with the Relevant Contract Records from the Data Module. The information required to prove or determine the amount of the refund is transmitted by the Provider to the relevant Contract Partner via the Contract Partner's access to the Lyfegen Platform in the form of a payment request in the name of the Customer, or otherwise in cases the Contract Partner has no access to the Lyfegen Platform. The Contract Partner is requested to pay the refund to either (a) to the Provider's account (separated from its other accounts, used only for funds of its customers) or (b) any other (e.g., third party) account, each as indicated on the Customer's power of attorney that has been issued for the Provider. In the case of (a), the Provider will within fifty [50] days transfer the funds, as received, with no interest, to the Customer's account on record, subject to fee deductions made as per the agreement. The Provider will regularly report to the Customer about its activities.

Annex 2: Security

1. **Definitions**

1.1. "**Best Industry Practice**" means, in relation to any undertaking or any circumstances, the exercise of the skill, care, diligence, prudence, foresight and judgement which would be expected from a suitably skilled, trained and experienced person operating to the standard that would be expected of a leading provider of services similar to the Lyfegen Platform, under the same or similar circumstances;

1. **IT Security**

2.1. In providing the Lyfegen Platform, the Provider has implemented data security procedures in accordance with Best Industry Practice.

2.2. The Provider has adopted, implemented, and shall maintain appropriate technical, organizational and physical security measures and takes all necessary precautions ("**Information Security Program**") pursuant to a comprehensive written information security program consistent with prevailing industry standards to:
2.2.1. preserve the integrity, security and confidentiality of Customer Data;
2.2.2. protect against any threats or hazards to the security or integrity of Customer Data;
2.2.3. prevent unauthorized or accidental processing, disposal, loss, destruction, theft, manipulation, interception or similar risks to Customer Data, having particular regard to:
2.2.3.1. any security measures incorporated (whether by automated means or otherwise) into the equipment in which Customer's Data is stored;
2.2.3.2. any measures taken for ensuring the integrity, prudence and competence of persons having access to Customer Data; and
2.2.3.3. any measures taken for ensuring the secure transmission of Customer Data;
2.2.4. take all necessary steps to ensure that no Virus is contained in or affects the Lyfegen Platform; and
2.2.5. keep Customer Data logically separate from other data and identify such data as the Customer's Confidential Information.

2.3. The Information Security Program includes at a minimum:
2.3.1. the implementation of access controls to prevent unauthorized access to or use of Customer Data, including access to the facilities in which Customer Data is Processed based on the following principles:
2.3.1.1. provision access to the Provider's personnel on a need to have and least privilege basis;
2.3.1.2. limit the Provider's personnel access to the information and services required to perform the respective job functions;
2.3.1.3. segregation of duties;
2.3.1.4. access is provided to the Provider's personnel only after they have been appropriately authorized;
2.3.1.5. an identifiable responsible person is associated with access credentials; and
2.3.1.6. access rights are promptly removed when no longer required.

2.3.2. appropriate approval and governance over the provisioning of emergency access to Customer Data;
2.3.3. knowledge to support, maintain and recover the Lyfegen Platform is sufficiently shared and documented between relevant personnel;
2.3.4. development, test and operational facilities are logically separated;
2.3.5. information security incident management shall be in place for the Lyfegen Platform;
2.3.6. technical vulnerability management shall be implemented for operating systems and any other applications in use in providing the Lyfegen Platform;
2.3.7. procedures for the management and secure destruction of removable media, including cryptographic controls in order to encrypt and guarantee the integrity of Customer Data, and controls to prevent unauthorized reading, copying, alteration or deletion of Customer Data during transportation of removable media containing Customer Data; and
2.3.8. controls are in place to prevent data leakage, including the protection of information exchange through the use of all types of communication facilities.

Annex 3: Support and Service Level Agreement

This Support and Service Level Agreement describes the Provider's support offerings in connection with the Customer's reported errors, defects and deficiencies in the Lyfegen SaaS Services, as well as the system availability targets that the Provider endeavors to maintain for the Lyfegen SaaS Services. All capitalized terms that are not defined in this Annex shall have the respective meaning given to such terms in the LTC.

1. **Definitions**

For the purpose of this Support and Service Level Agreement, the following terms shall have the following meaning:

1.1. "**Business Day**" means the total Business Hours in a support day.

1.2. "**Business Hours**" means 8:00am to 6:00pm CET, Monday through Friday, excluding local public holidays observed by the Provider (available upon request) and weekends.

1.3. "**Calendar Time**" is defined as the total number of Time in a given calendar month.

1.4. "**Customer Contact**" has the meaning set forth in Section 3.1.

1.5. "**Error**" means an error with a severity level 1, 2, 3, or 4, each as defined in the description column of Table A set out in Section 5.1.

1.6. "**Exceptions**" has the meaning set forth in Section 6.2.

1.7. "**Lyfegen Support**" has the meaning set forth in Section 2.1.

1.8. "**Monthly Subscription Fees**" means the subscription fees for the Lyfegen SaaS Services to be paid by the Customer to the Provider on a monthly basis as set forth in the applicable Work Order, or, if a yearly fee has been agreed in the applicable Work Order, the portion of such yearly fee that relates to the relevant month, which unless agreed otherwise shall be 1/12 of the (un-prorated) yearly fee.

1.9. "**Percentage Service Level Per Calendar Month**" is defined as the difference between the Calendar Time and the Unavailable Time, divided by Calendar Time, and multiplied by one hundred (100).

1.10. "**Service Level**" has the meaning set forth in Section 6.1.

1.11. "**Service Level Credits**" has the meaning set forth in Section 7.1.

1.12. "**Service Level Credit Request**" has the meaning set forth in Section 8.1.

1.13. "**Service Level Failure**" has the meaning set forth in Section 7.1.

1.14. "**Severity Level**" means one of the four Severity Levels 1, 2, 3, or 4, with 1 being the most critical severity and four 4 being the lowest critical severity, each as defined in the description column of Table A set out in Section 5.1.

1.15. "**Support Case**" has the meaning set forth in Section 3.1.

1.16. "**System Availability**" means the percentage of Calendar Time, where the application system processes supporting the Lyfegen Platform are running.

1.17. "**Table A**" means the Severity Level Response Time Target Table set out in Section 5.1.

1.18. "**Table B**" means the Service Level Credit Calculation Table set out in Section 7.1.

1.19. "**Time**" means one (1) hour.

1.20. "**Unavailable**" means when the application system processes supporting the Lyfegen Platform are not running.

1.21. "**Unavailable Time**" is defined as the total accumulated Time when the Service is Unavailable.

1. **Lyfegen Support Services**
   2.1. The Provider shall provide remote assistance to the Customer for questions or issues arising from any Errors, defects and deficiencies reported by the Customer in accordance with Sections 3 and 4 below that are not due to an Exception within the meaning of Section 6.2, including troubleshooting, diagnosis, and recommendations for potential workarounds for the duration of the Customer's subscription to the Lyfegen Platform (the "Lyfegen Support"). The Lyfegen Support is included in the Monthly Subscription Fees provided in the applicable Work Order.

2.2. However, the Provider will have no obligations to provide Lyfegen Support for third party software or services, custom scripts or code not native to the Lyfegen services. Additionally, technical or professional services from Lyfegen, including but not limited to services related to code development, migration or training are subject to a separate agreement between the Customer and the Provider and are expressly excluded from any Lyfegen Support services.

1. **Contacting Lyfegen Support**
   3.1. The Customer shall appoint and, in its reasonable discretion, replace, one and up to three customer employees to serve as the Customer's primary contact with respect to the Lyfegen SaaS Services, who will have the authority to act on behalf of the Customer in matters pertaining to the Lyfegen Support services, including the submission and processing of support requests (each a "**Customer Contact**"). The Customer Contacts may contact Lyfegen Support by submitting a support request to support@lyfegen.com or by calling the Provider's responsible customer success manager, and designating the appropriate severity level according to the Table A set out in Section 5.1 (each a "**Support Case**"). All Customer Contacts must be reasonably trained in the use and functionality of the Lyfegen Platform and shall use reasonable diligence to ensure a perceived Error is not due to any Exceptions as defined in Section 6.2.
2. **Submission of Support Cases**
   4.1. Each Support Case shall (a) designate the Severity Level of the Error based on the Customer's initial assessment, as described in Table A set out in Section 5.1 (b) identify the Customer account that experienced the error, (c) include information sufficiently detailed to allow Lyfegen Support to attempt to duplicate the Error (including any relevant error messages), and (d) provide contact information of

the Customer Contact most familiar with the issue. Unless Customer expressly designates the Severity Level, the Support Case will default to Severity Level 4.

3. **Error Response**
   5.1. Upon receipt of a Support Case, the Provider will attempt to determine the Error and assign the applicable Severity Level based on the descriptions provided in Table A. The Provider shall use commercially reasonable efforts to meet the Initial Response Time Target for the applicable Severity Level, as measured during the Support Hours set forth in Table A below. In exceptional cases at the Provider's discretion or if the Customer Contact who submitted the Support Case be unresponsive or unreachable, the Provider may downgrade the Severity Level by one level. Should the Provider's Severity Level designation be different from that assigned by the Customer, the Provider will promptly notify the Customer in advance of such designation. If the Provider notifies the Customer of a reasonable basis for disagreeing with the Customer's designated Severity Level, the Parties will discuss in an effort to come to a mutual agreement. If disagreement remains after discussion, each Party will escalate within its organization and use good faith efforts to mutually agree on the appropriate Severity Level.

Table A: Severity Level Response Time Target

Error Severity Level	**Description**	**Initial Response Time Target**	**Support Hours**
Severity Level 1 (Critical Severity)	An Error that (a) renders the Lyfegen services completely inoperative or (b) makes the Customer's use of material features of the Lyfegen services impossible, with no alternative available	Immediate, and in any event within thirty (30) minutes	24×7×365
Severity Level 2 (High Severity)	An Error that (a) has a high impact to key portions of the Lyfegen services or (b) seriously impairs the Customer's use of material function(s) of the Lyfegen services and the Customer cannot reasonably circumvent or avoid the Error on a temporary basis without the expenditure of significant time or effort	One (1) hour	24×7×365
Severity Level 3 (Medium Severity)	An Error that has a medium-to-low impact on the Lyfegen services, but the Customer can still access and use some functionality of the Lyfegen services	One (1) Business Day	Business Hours
Severity Level 4 (Low Severity)	An Error that has low-to-no impact on the Customer's access to and use of the Lyfegen services	One (1) Business Day	Business Hours

1. **Service Level**
   6.1. The Provider shall provide the Lyfegen SaaS Services to the Customer with a System Availability of at least 95% during each calendar month, excluding only the time the Lyfegen SaaS Services are not available solely as a result of one or more exceptions as defined in Section 6.2 ("Service Level").

6.2. The Provider will have no liability for any failure to meet the Service Level defined in Section 6.1, to the extent such failure arises from any of the following ("Exceptions"):
6.3. Use of the Lyfegen SaaS Services by the Customer and/or its authorized Users other than as authorized and intended under the Agreement and in accordance with the documentation;
6.4. Customer or User equipment;
6.5. Third party acts, services and/or systems not provided by the Provider pursuant to the Agreement and this Annex;
6.6. Internet access or capacity issues or other factors outside of the Provider's reasonable control;
6.7. Evaluation or proof-of-concept use of the Lyfegen services;
6.8. Scheduled downtime as notified by the Provider to the Customer at least five (5) Business Days in advance and to occur on weekends and holidays whenever possible; or
6.9. Suspension or termination of the Lyfegen SaaS Services pursuant to Sections 9 and 18 of the LTC or discontinuation of the provision of the Lyfegen Platform pursuant to Section 10 of the LTC

1. **Service Level Credit**

7.1. If the Lyfegen SaaS Services fail to meet the Service Level in a given month ("**Service Level Failure**"), then the Customer will be eligible to receive the applicable number of service credits set forth in Table B below ("**Service Level Credits**"), credited against the Customer's usage in the calendar month following the Service Level Failure, subject to the Customer's compliance with the credit request procedure set forth in Section 8 below. Service Level Credits may not be exchanged for, or converted to, monetary amounts, except upon termination of the Agreement pursuant to Section 18 of the Agreement.

Table B: Service Level Credit Calculation	
Percentage Service Level Per Calendar Month	Percentage Service Level Credit
Greater or equal to 95.00%	None
Under 95.00% but greater than or equal to 90.0%	10% of the Monthly Subscription Fee of the relevant month
Under 90.0% but greater than or equal to 85.0%	20% of the Monthly Subscription Fee of the relevant month
Under 85.0%	30% of the Monthly Subscription Fee of the relevant month

1. **Service Level Credit Request**
   8.1. Unless otherwise specified, the Customer's sole and exclusive remedy in the event of a Service Level Failure and the procedure for obtaining the Service Level Credits are as follows: (i) the Customer must submit a Service Level Credit request to the Provider by sending an email to support@lyfegen.com within twenty-one (21) days of the quarterly calendar in which the Service Level Failure occurred ("**Service Level Credit Request**"). The Service Level Request shall include (a) the date and duration of the System Availability failure, (b) any available supporting logs or records that corroborate the System Availability failure, (c) the affected Users and their locations and (d) any technical support requested or remediation implemented. Service Level Credit may be cumulated in a given month, but shall in any event not exceed 30% of the Monthly Subscription Fees. (ii) Upon confirmation by the Provider, the Customer will receive a Service Level Credit of the Monthly Subscription Fees in the amount calculated by the Provider in accordance with Table B above, applicable to its next invoice. (iii) In the event that the Customer disagrees regarding the System Availability failure or the Service Level Credit amount as determined by the Provider, the Customer shall provide written explanation of the disagreement to the Provider within fourteen (14) days of the Provider's response. The Provider shall respond in good faith with additional information or clarification and work through any discrepancies with the Customer.
2. **System Availability Monitoring and Reporting**
   9.1. The Provider shall continuously monitor and manage the Lyfegen SaaS Services to optimize System Availability that meets or exceeds the Service Level. Such monitoring and management shall include: (i) proactive monitoring of the Lyfegen SaaS Services functions, servers, firewall and other components of the service security and (ii) if such monitoring identifies, or the Provider otherwise becomes aware of, any circumstance that is reasonably likely to threaten System Availability, taking all necessary and reasonable remedial measures to promptly eliminate such threat and ensure full System Availability.

9.2. The Provider shall maintain records of System Availability at least at hourly intervals, which it shall make available upon request to the Customer.

ANNEX 4: PROCESSING OF CUSTOMER DATA AND OTHER PERSONAL DATA

1. **Data Module**

The Provider runs a SaaS, cloud-based platform to enable the Customer to record, manage and maintain patient data records ("**Data Module**"), and have selected data handed over to the Agreements Module. The following describes the Processing of Personal Data undertaken for the Data Module. It shall apply if and when a particular Work Order provides that the Provider shall provide the "Data Module" service to the Customer:

1.1. The categories of Data Subjects may include:
1.1.1. Patients;
1.1.2. Doctors, nurses and other personnel involved in the treatment of such patients;
1.1.3. Users.

1.2. The Personal Data Processed may include:
1.2.1. Customer Data
1.2.1.1. Personal details of patients, including name, gender, place and date of birth, age, insurance information, etc.;
1.2.1.2 Health data of patients, including health status, medical data (treatment information, treatment success, medication prescriptions, medical examination reports, laboratory tests, radiographs, etc.), administrative and financial information about health and treatments;
1.2.1.3. Names, functions, activities and other data of medical personnel involved in the treatments, testing and other recorded activities of the patient;
1.2.2. Usernames, passwords, permissions, requests, communications, activities of Users.

1.3. The Customer, as the Controller, instructs the Provider, as its Processor, to Process Customer Data for the term determined by the applicable Work Order and as otherwise set forth in the Agreement as follows:
1.3.1. Maintain patient records and other Customer Data provided for by the Users of the Customer;
1.3.2. Make available such patient records and other Customer Data to Users of the Customer;
1.3.3. Insofar agreed in the Work Order, hand over to the Agreements Module from the Customer Data records in the Data Module (selected by the Customer within the Data Module and at the intervals or events selected by the Customer within the Data Module) the data fields defined in the applicable Work Order ("from the Data Module" column of the Data-Driven Contract Record); the Customer shall configure, within the Data Module, the Data-Driven Contract to which the Customer Data handed over relates to in order for it to be properly assigned within the Agreements Module; within the Agreements Module, the Data-Driven Contract Record will be accessible to all parties of record to such Data-Driven Contract.

1.4. The Provider, as the Controller, may Process Personal Data of Users as necessary or useful and Customer Data as necessary to operate the Data Module beyond its role as a Processor (e.g., access control, logging, invoicing, support, statistics) and otherwise perform the Agreement or exercise its rights (including for archival/backup/documentary purposes), and for any other purpose required or permitted by applicable Law.

1. **Agreements Module and Sharing Module (if applicable)**

The Provider runs a SaaS, cloud-based platform that enables the Customer and its contracting partners to implement and execute "Data-Driven Contracts", including processing of patient data in accordance with the digital contract algorithms defined by them (for e.g. determining the final price of a medication) or having a patient's treatment progress analyzed with benchmark information shared with contracting partners of such Data-Driven Contract ("Agreements Module"). The following describes the Processing of Personal Data undertaken for the Agreements Module. It shall apply if and when a particular Work Order provides that the Provider shall provide the "Agreements Module" service to the Customer:

2.1. The categories of Data Subjects may include:
2.1.1. Patients;
2.1.2. Doctors, nurses and other personnel involved in the treatment of such patients;
2.1.3. Users.

2.2. The Personal Data Processed may include:
2.2.1. Customer Data. The main Customer Data to be Processed by the Provider for performing the Data-Driven Contracts as part of the Agreements Module service is agreed in the relevant Work Order ("Data-Driven Contract Record"). For the Provider, the Customer Data to be Processed in the context of the

Agreements Module may not necessarily qualify as Personal Data because the Provider is not able to identify the Data Subjects at issue. Nevertheless, the Parties agree to provide for the necessary governance and agreement in case such Customer Data were to qualify as Personal Data.

2.2.2. Usernames, passwords, permissions, requests, communications, activities of Users.

2.3. The Customer, as the Controller, instructs the Provider, as its Processor, to Process Customer Data for the term determined by the applicable Work Order and otherwise set forth in the Agreement as follows:
2.3.1. Accept, from the Data Module or any other agreed source, any Customer Data, in particular information on patient treatment and treatment results, that is provided to the Agreements Module for the Data-Driven Contract for which the relevant Work Order has been entered into;
2.3.2. Process such Customer Data as set forth by the Data-Driven Contract established by the Customer with its contracting partners and for which the Work Order has been entered into, including making available, based on such Customer Data, the relevant Data-Driven Contract Records to such contracting partners (e.g., payers, suppliers of medication) or, based on the Customer's specific instructions as available in the Sharing Module (where applicable), to the designated Receiving Partners;
2.3.3. Enable Customer to send and receive, within the Sharing Module (where applicable) communications (e.g., messages) to or from designated Receiving Partners as available within the Sharing Module;
2.3.4. Make available Customer Data to the Provider in its capacity as a Controller (in the case of records on patients for the purpose of Section 2.4.2 below only following their de-identification) (see below).

2.4. The Provider, as a Controller, may process:
2.4.1. Personal Data of Users as necessary or useful to operate the Agreements Module beyond its role as a Processor (e.g., access control, logging, invoicing, support, statistics) and otherwise perform the Agreement or exercise its rights (including for archival/backup/documentary purposes), and for any other purpose required or permitted by applicable Law.

2.4.2. Customer Data, including any Personal Data contained therein (in the case of records of patients for the purpose of Section 2.4.2.2 following their de-identification by the Customer), as follows:
2.4.2.1. As necessary to operate the Agreements Module beyond its role as a Processor (e.g., access control, logging, invoicing, support, statistics) and otherwise perform the Agreement or exercise its rights (including for archival/backup/documentary purposes).

2.4.2.2. For the purposes of any own use for the benefit of the Provider or a third party, as long as (a) such use is for statistical, research and development, benchmarking, archival and other purposes not related to particular individuals, and (b) any information made available to third parties (other than the Provider's service providers under a duty of confidentiality and the Provider's contracting partners (e.g., the suppliers of medication) engaged in the same Data-Driven Contracts) does (i) not contain Personal Data of patients or personnel involved in the treatment of such patients and (ii) not contain any information identifying the Customer;
2.4.2.3. For any other purpose required or permitted by applicable Law.

2.5. If the Agreements Module is provided to the Customer under several separate Work Orders but entered into under the same Agreement, the Agreements Module shall relate each Customer Data record to the relevant Work Order, but may permit the User, who is entitled to access such Customer Data, to see and manage it side-by-side to Customer Data records of other Work Orders and using the same login. Work Orders may be identified to the User through the names of the other customers of the Provider with which the relevant Data-Driven Contracts have been entered into by the Customer.

1. **RefaaS Services**

The Provider shall act as a Controller with regard to any personal data it may process for providing such services. The Customer hereby permits the Provider to access and process the Customer Data maintained by the Lyfegen Platform as necessary for, and for the purpose of, providing the RefaaS Services, and make updates to such Customer Data, as may be necessary to e.g. reflect refunds received.

ANNEX 5: LYFEGEN PLATFORM DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**Addendum**") shall form part of the Agreement made between the Customer and the Provider. In the event of a conflict or inconsistency, the terms of this Addendum shall supersede those of the rest of the Agreement insofar as it relates to data protection matters.

1. **Definitions**

1.1. In this Addendum the following terms shall have the meanings set out below:
1.1.1. "
Data Protection Impact Assessment" means an analysis of how Personal Data is collected, used, shared, protected and maintained, its impact on Data Subjects and measures undertaken to limit such impact, all pursuant to applicable Data Protection Legislation.

1.2. Other capitalized terms not defined in this Addendum have the meanings assigned to them in the LTC.

1. **Subject matter and duration of the Processing**
   2.1. The Provider acting as Processor on behalf of the Customer (Controller) collects, processes and stores Personal Data and shall do so only for the purposes of the Agreement or as otherwise directed in text by the Customer. In doing so, the Provider and the Customer shall comply with the Data Privacy and Security requirements set forth in this Addendum.

2.2. Unless otherwise agreed in text, the duration of the Processing corresponds to the duration of the Work Order or Agreement, as the case may be.

1. **Nature and purpose of the Processing**
   3.1. The nature and purpose of Processing Personal Data is further defined in the Agreement and respective service documentation.
2. **Type of Personal Data and categories of Data Subject**
   4.1. The categories of Data Subjects and the Personal Data collected, Processed and stored by the Provider is further defined in the Agreement and respective service documentation.
3. **Data Privacy**
   5.1. As the Controller, the Customer shall:
   5.1.1. Inform Data Subjects of his/her rights;
   5.1.2. Inform Data Subjects of the Personal Data collected and Processed in the context of the services provided by the Provider under this Agreement;
   5.1.3. Where necessary under applicable Data Protection Legislation ensure that there is a legal basis to Process Personal Data and, if the legal basis is consent of Data Subjects, collect and log the consent of Data Subjects associated to the collection, storage and Processing of his/her Personal Data and bear all costs and consequences in the case that the revocation of consent requires the Provider to amend its processing of the Personal Data;
   5.1.4. Communicate to the Provider the contact details of the security officer(s) and data protection officer(s).

5.2. The Customer warrants and undertakes towards the Provider that any Personal Data disclosed to the Provider within the framework of this Agreement was collected in a lawful way under the applicable Law and Data Protection Legislation and its Processing by the Provider does not in any way infringe upon the rights and freedoms of the Data Subject and/or third parties under the applicable Law and Data Protection Legislation. The Customer undertakes to promptly notify the Provider should it become aware that the Processing foreseen under this Agreement is not or no longer compliant with the applicable Law and Data Protection Legislation, including without limitation due to a change in the applicable Law and Data Protection Legislation.

5.3. As the Processor, the Provider shall:
5.3.1. Use all commercially reasonable endeavours to assist the Customer in its compliance with Data Protection Legislation, including without limitation the preparation of necessary notifications, registrations

and documentation which the Customer may be reasonably required to make or enter into in order to comply with Data Protection Legislation in connection with this Agreement;
5.3.2. Only process Personal Data upon documented lawful instructions from the Customer, unless otherwise required by applicable Law to which the Provider is subject. In such a case, the Provider shall inform the Customer of any such legal requirements before carrying out the required Processing, unless that Law prohibits such information on the basis of overriding public interests. The Customer agrees that the Agreement (including its Annexes, Appendixes and Annexes), the Provider's service documentation, along with the Customer's use and configuration of features in the services, are the Customer's complete and final documented instructions to the Provider for the Processing of Personal Data;
5.3.3. Have the processing Personal Data and the Lyfegen Platform hosted with the cloud hosting provider as set forth in Annex 5A and as per the terms listed therein. Any change of this setup as per the Customer's request shall be subject to the Provider's existing contractual commitments towards its respective subprocessor and subject to the Customer covering any additional costs due to such change. The Provider reserves the right to request a change of its cloud hosting provider at its own cost, and the Customer shall not unreasonably refuse such request;
5.3.4. Put in place measures to ensure:
5.3.4.1. that all employees who have access to Personal Data will not process such Personal Data beyond the instructions of the Customer, unless required to do so by applicable Law to which the Provider is subject; and
5.3.4.2. that all employees who have access to Personal Data are reliable and have committed themselves to confidentiality or are under a confidentiality obligation by operation of law.

5.3.5. Not disclose Personal Data to any other party without the Customer's express written agreement or express instruction;
5.3.6. Not transfer Personal Data to any location outside of Switzerland, the EEA or the country of the Customer unless:
5.3.6.1. the specific conditions of applicable Data Protection Legislation for such cross-border transfers of Personal Data have been fulfilled; or
5.3.6.2. such transfer is made to the Customer or to recipients instructed or indicated by the Customer, in which case, however, the Provider may require the Customer to enter into appropriate contractual safeguards if applicable Data Protection Legislation for such cross-border transfers of Personal Data requires so.

5.3.7. Subject to clause 5.3.3, commission subprocessors (additional contract processors) only after prior specific or general written or documented consent of the Customer.

5.3.7.1. The Customer agrees to the commissioning of the list of subprocessors attached to this Addendum as Annex 5A, under the condition that a contractual agreement in accordance with applicable Data Protection Legislation between Processor and such subprocessor has been concluded, subject to the specific provisions set forth in Annex 5A;
5.3.7.2. Further outsourcing to subprocessors or the change of existing subprocessors is agreed by the Customer subject to (1) the Provider submitting such an outsourcing to a subprocessor in writing or in text form (including a post on the platform of the Provider or its subprocessors, with making available to the Customer a method of being notified of changes) to the Customer with 30 days prior notice; (2) the Customer not objecting to the planned outsourcing in writing or in text form within 20 days; and (3) the subprocessing being based on a contractual agreement in accordance with applicable Data Protection Legislation.

5.3.8. Promptly notify the Customer if the Provider receives a request from a Data Subject to have access to Personal Data or exercise any other applicable Data Subject rights, and assist the Customer insofar as reasonably possible in responding to any such request or complaint, including, without limitation:
5.3.8.1. where authorized by the Customer, by allowing the Data Subject to have access to his/her Personal Data or to have that Personal Data corrected, deleted, or blocked within the relevant timeframes set out by the applicable Law;

5.3.8.2. by providing the Customer with any requested information relating to the Processing of Personal Data under this Addendum;
5.3.8.3. by providing the Customer with any Personal Data the Provider holds in relation to a Data Subject, if required in a commonly used, structured, electronic and machine-readable format;
5.3.9. If the Customer is obliged by Data Protection Legislation to carry out a data protection impact assessment in relation to the services provided by the Provider under this Agreement, the Provider will reasonably support the Customer in carrying out such data protection impact assessment to the extent reasonably possible;
5.3.10. Permit the Customer (or the duly authorized representatives or any regulator to which the Customer is subject) to inspect and audit the Provider Processing activities under this Agreement (and/or those of any of its agents or subprocessors, subject to their restrictions insofar such restrictions are in line with applicable Data Protection Legislation, including as per Annex 5A), and comply with all reasonable requests or directions by Customer to enable them to verify and/or confirm that the Provider is in full compliance with its obligations under this Agreement;
5.3.11. Immediately inform Customer if in the Provider's opinion one of the Customer's instructions infringes the provisions of applicable Data Protection Legislation;
5.3.12. If so requested by Customer at any time, provide Customer with a copy of the Personal Data or (at Customer's option) destroy it, save where applicable Law requires the Provider to retain copies of such Personal Data; and
15.3.3. Upon termination of the Provider's provisions of services relating to Personal Data, delete or return all Personal Data to Customer and delete any existing copies of such Personal Data, save where applicable Law requires the Provider to retain copies of such Personal Data.

5.4. The Provider may claim reasonable compensation for all costs incurred in connection with its support to Controller, inspections or audits by Controller and other obligations pursuant to Annex 5 not expressly included in the charges of the services to be provided pursuant to the Agreement.

1. **Security**
   6.1. The Customer is responsible for the proper creation and management of its user accounts, including the deactivation and review of its user accounts. The Customer shall in particular ensure that:
   6.1.1. Access and authorizations are granted on a "need to have" basis;
   6.1.2. Each User is assigned a unique account;
   6.1.3. Accounts are periodically reviewed to validate their relevance;
   6.1.4. Generic accounts are not used;
   6.1.5. Passwords contain at least 8 characters consisting of a combination of characters, numbers and symbols;
   6.1.6. Accounts suspected of being compromised are immediately deactivated.

6.2. The Provider shall:
6.2.1. Implement and maintain appropriate technical and organizational measures to ensure the security and protection of Personal Data, including during the transmission, taking into account the nature and sensitivity of the information to be protected, the risk presented by the Processing, the state of the art, and the costs of implementation, in accordance with applicable Data Protection Legislation. Such measures shall include appropriate physical, electronic and procedural safeguards to (a) ensure the security, confidentiality and integrity of Personal Data made available to it and (b) protect Personal Data against unauthorized access or disclosure, accidental or unlawful destruction or accidental loss or alteration;
6.2.2. Maintain and enforce the security measures set forth in Technical and Organizational Measures provided in Annex 5B to this Addendum.

6.2.3. Promptly notify the Customer as soon as the Provider becomes aware of a data breach as defined by the GDPR or other Data Protection Legislation applicable to Processor ("**Data Security Breach**").

6.2.4. In the event of a Data Security Breach, (a) immediately investigate, correct, mitigate, remediate and otherwise address the Data Security Breach, including without limitation, by identifying the Personal Data affected by the Data Security Breach and taking reasonable steps to prevent the continuation and recurrence of the Data Security Breach; and (b) provide information and assistance as necessary to enable the Customer to evaluate the Data Security Breach and, where appropriate, to provide timely notices of disclosure of a Data Security Breach and comply with any obligations to provide information about the Data Security Breach to the relevant supervisory authority.

Annex 5a: Subprocessors

The Customer agrees to the commissioning of the following subprocessors of Lyfegen HealthTech AG:

Company	**Address/Country**
Microsoft Ireland Operation Ltd.	Ireland
Service	
Cloud Infrastructure and Platform Services. Lyfegen primarily uses Microsoft Azure's Swiss-based cloud infrastructure, which is HIPAA compliant. Lyfegen reserves itself the right to change Cloud Infrastructure provider; if HIPAA/HITECH is applicable, as specified in the Work Order, Lyfegen has only the right to change Cloud Infrastructure provider to another HIPAA compliant product.Provider has engaged this subprocessor as per the subprocessor's standard data processing and security terms as published here (and as may be amended from time to time): https://azure.microsoft.com/en-us/support/legal/With regard to any Processing of Personal Data by, and any other activities of or related to this subprocessor, the subprocessor's terms shall apply instead of any broader or further obligations of Processor under this Data Processing Addendum or the Agreement, including as to the use of further subprocessors by such subprocessor. Customer agrees to track, as it deems necessary, the changes of Microsoft's subprocessors as announced by Microsoft.	

If Lyfegen HealthTech AG itself is not the Provider, the Customer agrees to the commissioning of the following additional subprocessors:

Company	**Address/Country**
Lyfegen HealtTech AG	Aeschenvorstadt 57, 4051 Basel, Switzerland
Service	
Provision of the Lyfegen Platform and support services.	

Annex 5B: Technical and Organizational Measures OF SECURITY

Capitalised terms not otherwise defined in this document have the meanings assigned to them in the Agreement or the Data Processing Addendum.

1. **Information Security Program**

1.1. The Provider will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help the Customer secure Personal Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorised access to the Lyfegen Platform, and (c) minimize security risks, including through risk assessment and regular testing. The Provider will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the measures set forth in Sections 2 and 3 below.

1. **Network Security**
   2.1. The hosted environment and network on which the Lyfegen Platform is deployed is electronically accessible to employees, contractors and any other person as necessary to provide the Lyfegen Platform. The Provider maintains access controls and policies to manage which access is allowed to

the Lyfegen Platform and the hosted environment from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. The Provider maintains corrective action and incident response plans to respond to potential security threats.

2. **Physical Security**
   3.1.
   Physical Access Controls. Physical components of the hosted environment on which the Lyfegen Platform is deployed are housed in nondescript facilities including facilities of subprocessors (the "**Facilities**"). Physical barrier controls are used to prevent unauthorised entrance to the Facilities both at the perimeter and building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Visitors are required to sign-in with designated personnel, must show appropriate identification, and are continually escorted by authorised employees or contractors while visiting the Facilities.

3.2. **Limited Employee and Contractor Access.** The Provider provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or a contractor no longer has a business need for the access privileges assigned to him/her, the access privileges will be promptly revoked, even if the employee or the contractor continues to be an employee of the Provider or its subprocessors.

1. **Continued Evaluation**
   4.1. The Provider will conduct periodic reviews of the security of the Lyfegen Platform and the adequacy of its information security program as measured against industry security standards and its policies and procedures. The Provider will continually evaluate the security of the Lyfegen Platform and associated services to determine whether additional or different security measures are required to address new security risks or findings from the periodic reviews.

Annex 6: BUSINESS ASSOCIATE PROVISIONS

For purposes of this Annex 6, Customer is referred to as the "Covered Entity" and Provider is referred to as the "Business Associate" (each a "Party" and collectively the "Parties"). To the extent applicable and required by applicable Law, this Annex accompanies and is incorporated into the Agreement.

1. **Background**

1.1. Business Associate performs functions, activities or services for, or on behalf of Covered Entity and Business Associate receives, has access to or creates Protected Health Information ("PHI"), including Electronic Protected Health Information ("EPHI"), in order to perform such functions, activities or services. The purpose of these Business Associate Provisions (referred to herein as the"BAA") is to set forth the terms and conditions of disclosure of PHI by Covered Entity to Business Associate, to set forth the terms and conditions of Business Associate's use and disclosure of Protected Health Information, and to ensure the confidentiality, integrity and availability of EPHI that Business Associate creates, receives, maintains or transmits on behalf of Covered Entity. Covered Entity and Business Associate intend to protect the privacy and provide for the security of PHI disclosed to Business Associate pursuant to the Subscription Agreement in compliance with (i) the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"); (ii) Subtitle D of the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), also known as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009; (iii) regulations promulgated thereunder by the U.S. Department of Health and Human Services, including the HIPAA Omnibus Final Rule (the "HIPAA Final Rule"), which amended the Privacy Rule and the Security Rule (as those terms are defined below) pursuant to the HITECH Act, extending certain HIPAA obligations to business associates and their subcontractors, and (iv) State Privacy and Security Laws
2.
Definitions

Terms used, but not otherwise defined, in this BAA shall have the same meaning as those terms in the Privacy Rule and Security Rule promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996. 45 CFR Parts 160 and 164.

2.1. "**ARRA**" shall mean the American Recovery and Reinvestment Act of 2009, Public Law 111-5.

2.2. "**Breach**" shall have the same meaning given to such term in 45 C.F.R. § 164.402.

2.3. "**Electronic Health Record**" or "**EHR**" means a digital, patient-centered record focused on the total health of the patient and built to share patient information with other health care providers and organizations.

2.4. "**Electronic Medical Record**" or "**EMR**" means a digital record of medical and treatment history of the patients within one health care organization.

2.5. "**Electronic Protected Health Information**"or "**EPHI**" shall have the same meaning as the term "electronic protected health information" in 45 CFR § 160.103, but shall be limited to the EPHI that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity.

2.6. "**Encrypted**" means data is encrypted in compliance with the U.S. Department of Health and Human Services Guidance specifying the Technologies and Methodologies that render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of HITECH Act.

2.7. "**Electronic Health Record**"or "**EHR**" means a digital, patient-centered record focused on the total health of the patient and built to share patient information with other health care providers and organizations.

2.8. "**Electronic Medical Record**"or "**EMR**" means a digital record of medical and treatment history of the patients within one health care organization.

2.9. "**HIPAA Law**" shall mean the Privacy Rule, the Security Rule, the HITECH Act, ARRA, and the HIPAA Final Rule.

2.10. "**Individual**" shall have the same meaning as the term "individual" in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

2.11. "**Limited Data Set**" shall have the same meaning as a "limited data set" described in 45 CFR § 164.514(e)(2).

2.12. "**Minimum Necessary**" shall have the same meaning as "minimum necessary" described in 45 CFR § 164.502(b).

2.13. "**Privacy Rule**" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and Part 164, subparts A and E.

2.14. "**Protected Health Information**" or "**PHI**" shall have the same meaning as the term "protected health information" in 45 CFR § 160.103, but shall be limited to the information created or received by Business Associate from or on behalf of Covered Entity.

2.15. "**Required By Law**" shall have the same meaning as the term "required by law" in 45 CFR § 164.103.

2.16. "**Secretary**" shall mean the Secretary of the United States Department of Health and Human Services or his designee.

2.17. "**Security Incident**" shall have the same meaning as "security incident" in 45 CFR § 164.304.

2.18. "**Security Rule**" shall mean the Security Standards for the Protection of EPHI at 45 CFR Parts 160 and 164, subparts A and C.

2.19. "**State Privacy and Security Laws**" shall mean all applicable state laws relating to privacy, security, data breach and confidentiality of the information provided to Business Associate under this Agreement.

2.20. "**Unsecured PHI**" shall have the same meaning given to such term under 45 C.F.R. § 164.402, and guidance promulgated thereunder.

2.21. "**Unsuccessful Security Incidents**" shall mean pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of PHI.

1. **Permitted uses and disclosures by Business Associate**
   3.1. General Use and Disclosure. As between Covered Entity and Business Associate, any PHI disclosed, delivered or provided to Business Associate, shall be deemed to be the exclusive property of Covered Entity. Except as otherwise limited in this BAA, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Subscription Agreement, or other agreements entered into between the Covered Entity and Business Associate, or as otherwise permitted by applicable Law provided that such use or disclosure would not violate the Privacy Rule, or the Security Rule if done by Covered Entity. Except as otherwise limited in this BAA, Business Associate agrees to not use or further disclose PHI other than as permitted or required by the Subscription Agreement or as Required By Law. All uses and disclosures of PHI must comply with the minimum necessary requirements under the Privacy Rule as well as any additional guidance or regulations issued by the Department of Health and Human Services. The Party disclosing PHI shall determine what constitutes the minimum necessary to accomplish the intended purpose of the disclosure. Until the effective date of further guidance or regulations issued on the meaning of minimum necessary, Business Associate shall use a Limited Data Set when using, disclosing, and requesting PHI, to the extent practicable. Any use, disclosure, or request of PHI must be limited to the Minimum Necessary to accomplish the intended purpose of the use, disclosure, or request. After the effective date of subsequent implementing guidance and/or regulations on the meaning of Minimum Necessary, Business Associate shall comply with such guidance or regulations.

3.2. Specific Use and Disclosure.

3.2.1. Except as otherwise limited in this BAA, Business Associate may use or disclose PHI for the proper management and administration of Business Associate, provided that disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it becomes aware in which the confidentiality of the information has been breached.

3.2.2. Business Associate may use PHI to report violations of law to appropriate state and federal authorities, to the extent permitted or required by 45 CFR § 164.502(j)(1) and state law.

4.2. **Obligations and activities of Business Associate**
4.2.1. Use and Disclosure. To the extent Business Associate is carrying out any of Covered Entity's obligations under the Privacy Rule pursuant to the terms of the Subscription Agreement or this BAA, Business Associate shall also comply, where applicable, with 45 CFR Part 164 Subpart C with respect to EPHI, and the use and disclosure provisions of the Privacy Rule. Additionally, Business Associate is authorized to use or disclose any and all PHI and other data provided to it by Company for internal purposes of product improvement, reporting, benchmarking, and tracking or similar usage. Business Associate is further permitted to use or disclose PHI for the purpose of developing information or statistical compilation for use by third parties provided that such use or disclosure is not prohibited by applicable law. Upon Covered Entities' written request, Business Associate agrees to provide an annual written attestation of its compliance to the HIPAA Law in a form and format provided at the discretion of the Covered Entity in order to obtain satisfactory assurances in accordance with the HIPAA Law that the Business Associate will appropriately safeguard the information with which it is entrusted.

4.2.2. Safeguards. Business Associate agrees:
4.2.2.1. To use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by this BAA.

4.2.2.2. To develop, implement, maintain, and use appropriate administrative, technical, and physical safeguards to reasonably and appropriately protect the confidentiality, integrity, and availability of EPHI that Business Associate creates, receives, maintains or transmits on behalf of Covered Entity. Such administrative, technical, and physical safeguards must meet the requirements outlined at 45 CFR Part 164 Subpart C. Business Associate shall document and keep these security measures current in accordance with 45 CFR § 164.316. Any hard drives on any computers or laptops that are used to access, receive, send, or maintain Covered Entity's EPHI must be Encrypted and all communications must be Encrypted if sending EPHI over an open network. Mobile devices or external or removable media, including, without limitation backup tapes, used for sending, receiving, or storing EPHI must be Encrypted and password protected.

4.2.2.3. That it is obligated by law to meet the provisions of the Privacy Rule and the Security Rule that are applicable to business associates.

4.2.3. Subcontractors. Business Associate agrees to ensure that any subcontractor that creates, receives, maintains, or transmits PHI (including EPHI) on behalf of the Business Associate agrees to the same restrictions and conditions that apply through this BAA to Business Associate with respect to such information, including but not limited to, compliance with the applicable requirements of 45 CFR Parts 160 and 164. Such agreement between Business Associate and the subcontractor must be made in writing and must comply with the terms of this BAA and the requirements outlined in 45 CFR §§ 164.504(e) and 164.314.

4.4. Designated Record Set.

4.1. If Business Associate has PHI in a Designated Record Set, Business Associate agrees to provide access within fifteen (15) calendar days, at the written request of Covered Entity, to PHI in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR § 164.524. If an Individual makes a request for access pursuant to 45 C.F.R. § 164.524 directly to Business Associate, or inquires about his or her right to access, Business Associate shall direct the Individual to Covered Entity. If Business Associate uses or maintains an electronic health record with respect to PHI of an Individual, Business Associate agrees to provide a copy of such information in an electronic format and to transmit such copy to an entity or person designated by Covered Entity. Business Associate shall be entitled to impose a reasonable fee for such copies and transmittal.

4.2. Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 CFR § 164.526 at the request of Covered Entity or an Individual, within fifteen (15) calendar days after a request and in the manner designated by Covered Entity.

4.3. Business Associate agrees to promptly notify Covered Entity of any amendments and await approval.

4.5. Internal Practices.

4.5.1. Business Associate agrees to make internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI or EPHI received from, or created or received by Business Associate on behalf of, Covered Entity reasonably available to Covered Entity, or to the Secretary, in a time and manner reasonably selected by Covered Entity or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule. Any such audit shall be limited to data files that are specific to Covered Entity, and shall not interfere with the data, confidentiality, or intellectual property of Business Associate's other clientele or unduly interfere with the operations of Business Associate.

4.5.2. Business Associate agrees to make internal practices, books, and records, including policies and procedures, relating to the security of EPHI created, received, maintained, or transmitted by Business Associate on behalf of, Covered Entity reasonably available to Covered Entity, or to the Secretary, in a time and manner reasonably selected by Covered Entity or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Security Rule. Any such audit shall be limited to data files that are specific to Covered Entity, and shall not interfere with the data, confidentiality, or intellectual property of Business Associate's other clientele or unduly interfere with the operations of Business Associate.

4.6. Documentation of Disclosures.

4.6.1. Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. Beginning on the effective date of Section 13405(c) of ARRA, if Business Associate uses or maintains an electronic health record with respect to PHI, Business Associate agrees to document disclosures made through an electronic health record for treatment, payment, or health care operations, and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures in accordance with 45 C.F.R. § 164.528.

4.6.2. Business Associate agrees to promptly provide written notification to Covered Entity or an Individual, in not more than fifteen (15) calendar days after a request and in the manner designated by Covered Entity, information collected in accordance with Section 8.9 of this BAA prior to Business Associate taking action, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528.

4.7. Prohibition on the Sale of PHI or Electronic Health Records. Business Associate shall comply with 45 CFR § 164.502(a)(5), which relates to the prohibition on the sale of Electronic Health Records and PHI.

4.8. Conditions on Certain Marketing and Fundraising Contacts. Business Associate shall not use or disclose PHI for marketing or fundraising without consent of Covered Entity and only to the extent permitted by 45 CFR §§ 164.508(a)(3) and 164.514(f).

4.9. Business Associate's Obligations Related to Breach of Unsecured PHI.

4.9.1. Reports of Security Incidents. Business Associate agrees to promptly report to Covered Entity any Security Incident of which it becomes aware, without unreasonable delay, and in any event no more than five (5) days following discovery. The Parties acknowledge and agree that this Section constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined above) for which notice to Covered Entity by Business Associate shall be required only upon request.

4.9.2. Breach. Business Associate will report to Covered Entity any use or disclosure of Covered Entity's PHI that is not permitted by this BAA or Applicable Law. In addition, Business Associate will report to Covered Entity following discovery and without unreasonable delay, but in no event later than ten (10) days following discovery of any suspected or actual Breach of Unsecured Protected Health Information or any actual or suspected disclosure or inappropriate access of Covered Entity's information which is subject to state privacy or security breach laws. Business Associate shall cooperate with Covered Entity in investigating the potential or actual breach, disclosure or inappropriate access and in meeting Covered Entity's obligations under the HITECH Act and any other state or federal privacy or security breach notification laws. Any such report shall contain at a minimum the information set forth on Exhibit C1 attached hereto and incorporated by reference. To the extent any Breach of Unsecured Protected Health Information or unauthorized acquisition or access to information subject to State Privacy and Security Laws is solely attributable to: (i) a material breach of the obligations under this BAA by Business Associate or its employees, agents or subcontractors, (ii) a violation of the HIPAA Law or State Privacy and Security Laws by Business Associate, or its employees, agents or subcontractors, or (iii) Unsecured PHI in Business Associate's possession, or PHI created, maintained, transmitted, or received by Business Associate or its employees, agents, representatives, or subcontractors, then Business Associate shall bear the reasonable costs incurred by Covered Entity in complying with its legal obligations relating to such breach or violation, subject to any liability limitations agreed by the Parties. Business Associate shall not be liable for the following expenses incurred by Covered Entity in responding to such breach: (1) the cost of preparing and distributing notifications to affected Individuals, (2) the cost of providing notice to government agencies, credit bureaus, and/or other required entities, (3) the cost of providing affected

Individuals with credit monitoring services, to the extent the incident involved financial information, (4) call center support for such affected Individuals and (5) the cost of any other measures required under applicable law.

4.9.3. In addition to the information required in Exhibit C1, Business Associate's notice shall include, to the extent possible, the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, used, or disclosed during or as a result of the Breach. Business Associate shall also provide Covered Entity with at least the following information: a description of the Breach, if known; a description of the types of Unsecured PHI involved in the Breach; any steps Individuals should take to protect themselves from potential harm resulting from the Breach; a brief description of what Business Associate is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any further Breaches; and any other information requested by Covered Entity related to the Breach. Business Associate shall promptly supplement such notice with additional information as it becomes available, even if such information becomes available after Individuals have been notified of the Breach.

4.9.4. Mitigation. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this BAA.

4.10. Notification of Governmental Audit. Business Associate agrees to promptly notify Covered Entity if it is the subject of a HIPAA compliance/enforcement audit by the Department of Health and Human Services Office of Civil Rights and to promptly notify Covered Entity of any findings of such audit that impact the services provided by Business Associate to Covered Entity.

4.11. Government Program Requirements. To the extent that Business Associate receives, uses or discloses PHI pertaining to Individuals enrolled in managed care plans through which Customer or one or more of its affiliates participate in government funded health care programs, receipt, use and disclosure of the PHI pertaining to those individuals shall comply with the applicable program requirements.

4.12. Substance Use Disorder Program Requirements. To the extent that Business Associate receives, uses, or discloses PHI pertaining to Individuals with respect to substance use disorder records, Business Associate agrees to abide by 42 CFR § 290dd-2.

5.3. **Obligations of Covered Entity**

5.3.1. Privacy Practices. Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with 45 CFR § 164.520, as well as any changes to such notice, to the extent that such limitation may affect Business Associate's uses or disclosure of PHI.

5.3.2. Notice of Changes and Restrictions. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose PHI, to the extent such changes affect Business Associate's permitted or required uses and disclosures. Such notification shall include any restriction that Covered Entity has agreed to in accordance with 45 CFR § 164.522. If Business Associate receives a request to restrict the disclosure of PHI directly from an Individual, Business Associate shall notify Covered Entity of such request and Covered Entity shall be responsible for making the determination, in accordance with the Privacy Rule, as to whether Business Associate shall comply with the Individual's request. If any restriction agreed to by Covered Entity pursuant to this Section prevent Business Associate's from performing its obligations under the Subscription Agreement or this BAA, Business Associate shall be excused from performing obligations which are so impaired.

5.3.3. Permissible Requests by Covered Entity. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule or the Security Rule if done by Covered Entity, except that Business Associate is permitted to use or disclose PHI for data aggregation or management and administrative activities of Business Associate and as otherwise set out in this BAA.

1. **Term and Termination**
   6.1. Term. This BAA shall be effective upon execution of the Subscription Agreement by the Parties and shall remain in effect for the duration of the Subscription Agreement, relationship, functions or services giving rise to the necessity of a Business Associate Agreement, and until all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this Section.

6.2. Termination.

6.2.1. Termination Resulting from the End of Relationship, Functions or Services. This BAA shall terminate in the event that the Subscription Agreement, underlying relationship, functions, or services that give rise to the necessity of a Business Associate Agreement terminate for any reason.

6.2.2. Termination for Cause. Upon either Party's knowledge of a material breach of this BAA by the other Party, the non-breaching Party must either Provide an opportunity for the breaching Party to cure the breach or end the violation, and if the breaching Party does not cure the breach or end the violation within the time specified by the non-breaching Party; provided such time is no less than ten (10) calendar days, the non-breaching Party shall terminate this BAA and, at its election, any Subscription Agreement or agreements, if cure is not possible;
6.3. Return or Destruction of PHI.

6.3.1. Except as provided in Section 6.3.2, upon termination of this BAA, for any reason, Business Associate shall return or destroy (at Covered Entity's sole discretion) all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity within fifteen (15) calendar days of the effective date of the termination. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall not retain any copies of the Protected Health Information. Business Associate will be responsible for recovering any PHI from such agents or subcontractors at no cost to Covered Entity. Any information that is in electronic format shall be provided to Covered Entity at no additional charge. The format to be provided should be one that is commonly used for export (i.e. comma delimited, text file, Word, Excel or Access database) that is agreeable to Covered Entity.

6.3.2. In the event that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity written notification of the conditions that make return or destruction infeasible. If such written notification that return or destruction of Protected Health Information is infeasible is provided to and agreed by Covered Entity, Business Associate shall extend the protections of this BAA to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

6.3.3. In addition to rights of termination set forth in Section 6.2 should Business Associate make a disclosure of PHI in violation of this BAA, Covered Entity shall have the right to immediately terminate any contract, then in force between the Parties, including any Subscription Agreement.

1. **Indemnification**
   7.1. Business Associate will indemnify, defend and hold Covered Entity and its officers, directors, employees, agents, affiliates, successors and assigns harmless, from and against any and all losses, liabilities, damages, costs, penalties, fines and expenses (including reasonably attorneys' fees and costs) arising out of or related to either: (i) the Business Associate's breach of its obligations under this Agreement and/or (ii) any third-party claim based upon any breach of this Agreement, violation of HIPAA Laws or State Privacy and Security Laws by Business Associate or by its employees, agents or subcontractors ("Claim"). If Business Associate assumes the defense of a Claim, Covered Entity shall have the right, at its sole expense, to participate in the defense of such Claim, and Business Associate shall not take any final action with respect to such Claim without the prior written consent of Covered

Entity. This Section shall survive termination of this Agreement and any Claim is subject to any limitation or exclusion of damages or liability provisions otherwise set forth in any underlying agreement.

7.2. Covered Entity will indemnify, defend and hold Business Associate and its officers, directors, employees, agents, affiliates, successors and assigns harmless, from and against any and all losses, liabilities, damages, costs, penalties, fines and expenses (including reasonably attorneys' fees and costs) arising out of or related to either: (i) the Covered Entity's breach of its obligations under this Agreement and/or (ii) any third-party claim based upon any breach of this Agreement, violation of HIPAA Laws or State Privacy and Security Laws by Covered Entity or by its employees, agents or subcontractors ("Claim"). If Covered Entity assumes the defense of a Claim, Business Associate shall have the right, at its sole expense, to participate in the defense of such Claim, and Covered Entity shall not take any final action with respect to such Claim without the prior written consent of Business Associate. This Section shall survive termination of this Agreement and any Claim is subject to any limitation or exclusion of damages or liability provisions otherwise set forth in any underlying agreement.

1. **Miscellaneous**
   8.1. Regulatory References. A reference in this BAA to a section in the Privacy Rule, the Security Rule, or ARRA, or any other reference to a law or regulation, means the section or law as in effect as of the date of this BAA or as subsequently amended.

8.2. Amendment. The Parties agree to take such action as is necessary to amend this BAA from time to time to comply with the requirements of the Privacy Rule, the Security Rule, HIPAA, and ARRA
8.3. Survival. The respective rights and obligations of Business Associate under Sections 4.10, and 6.3 of this BAA shall survive the termination of this BAA.

8.4. Interpretation. Any ambiguity in this BAA shall be resolved in favor of a meaning that permits compliance with the Privacy Rule, the Security Rule, and ARRA.

8.5. Relationship to Other Agreement Provisions. In the event that a provision of this BAA is contrary to a provision of the Subscription Agreement or agreements under which Covered Entity discloses PHI to Business Associate, the provision of this BAA shall control. Otherwise, this BAA shall be construed under, and in accordance with, the terms of such Subscription Agreement or agreements between the Parties.

8.6. Prior Business Associate Agreements. Consistent with Section 8.5, this BAA shall supersede any and all prior business associate agreement(s), or terms of other agreements addressing the privacy and security of PHI, between the Parties. This BAA is the complete and exclusive agreement between the Parties with respect to the subject matter hereof, superseding and replacing all prior agreements, communications and understandings (written and oral) regarding its subject matter.

8.7. Modification of Agreement. No alteration, amendment or modification of the terms of this BAA shall be valid or effective unless in writing and signed by Business Associate and Covered Entity.

8.8. Compliance with State Law. Business Associate shall comply with State Privacy and Security Laws. If the HIPAA Privacy or Security Rules and the law of the State in which Covered Entity is located conflict regarding the degree of protection provided for protected health information, Business Associate shall comply with the more restrictive protection requirement.

8.9. Notices. Any notices required or permitted to be given under this BAA by either Party shall be given in writing: (a) by personal delivery; (b) by electronic facsimile with confirmation sent by United States first class mail; (c) by bonded courier or nationally recognized overnight delivery service; or (d) by United States first class registered or certified mail, postage prepaid, return receipt requested, addressed to the Parties at the addresses specified in the Work Order or to such other addresses as the Parties may request in writing by notice pursuant to this Section 8.9 Notices shall be deemed received on the earliest of personal delivery, upon the next business day after delivery by electronic facsimile with confirmation that the transmission was completed or upon receipt by any other method of delivery