Data Processing Agreement (DPA)

To the extent Capsa Processes Personal Data on Distributor's behalf, this Data Processing Agreement ("**DPA**") applies. All capitalized terms not otherwise defined in this DPA will have the meaning given to them in the Agreement. If there is any inconsistency or conflict between this DPA and the Agreement as it relates to data protection, this DPA will govern. To the extent Capsa Processes Personal Data on behalf of Distributor, Distributor and Capsa agree as follows:

1. DEFINITIONS

1.1. "**Data Protection Requirements"** means all applicable laws, rules, regulations, orders, ordinances, and regulatory guidance related to privacy and data security and the Processing of Personal Data, including, but not limited to the GDPR.

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

1.3. "**Security Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by Capsa on behalf of Distributor.

1.4. "**Services**" means any services Capsa provides to Distributor under the Agreement or any Statement of Work, including, but not limited to, any hosting services or support services.

1.5. "**Standard Contractual Clauses**" means standard contractual clauses, as approved by the European Commission, for the transfer of personal data to Processors established in third countries that do not ensure an adequate level of protection as set out in Commission Decision C(2010) 593, which are available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en, as updated, amended, approved, replaced or superseded from time to time by the European Commission or other authorized authority.

1.6. "**Supervisory Authority**" shall have the meaning assigned to it in the GDPR, unless another Data Protection Requirement governs the Personal Data, in which case the definition of the governmental body authorized to enforce such Data Protection Requirement shall apply.

1.7. The terms "**Controller**," "**Data Subject**," "**Personal Data**," "**Process**" or "**Processing**," and "**Processor**" will have the meanings given to them under the GDPR.

2. DATA PROCESSING

2.1. Processing Purpose and Instructions. Distributor and Capsa agree that Distributor is the Processor of Personal Data and Capsa is a subprocessor. In performing its obligations under the Agreement, Capsa will Process Personal Data on Distributor's behalf. Capsa will Process Personal Data on behalf of Distributor to provide the Services pursuant to Distributor's documented instructions. Annex 1 describes the subject matter and details of such Processing.

2.2. Processing in Compliance with Applicable Law. Capsa may Process Personal Data for purposes other than those set forth in Distributor's written instructions if applicable law requires Capsa to do so. In this situation, Capsa shall inform Distributor of such requirement before Capsa Processes the Personal Data, unless prohibited by applicable law. Each party will comply with the obligations applicable to it under the Data Protection Requirements with respect to Processing Personal Data.

2.3. Distributor Obligations. Distributor instructs Capsa to Process Personal Data on behalf of Distributor in accordance with the Agreement. Distributor shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Distributor obtained the Personal Data. Distributor represents and warrants that Distributor has a lawful basis for Processing Personal Data and that Distributor has provided the required notices and obtained the requisite consent from the Controller to Process Personal Data. Distributor represents and warrants to Capsa that Distributor's instructions and actions with respect to Personal Data, including Distributor's appointment of Capsa as another Processor, have been authorized by the Controller and comply with Data Protection Requirements.

2.4. Sensitive Personal Data. Distributor authorizes Capsa to Process sensitive Personal Data on behalf of Distributor, including but not limited to biometric data and data concerning a Data Subject's health and medical information. Distributor shall have the sole responsibility to provide all legally-required notices and obtain all legally-required consents necessary for Capsa to Process sensitive Personal Data on behalf of Distributor.

3. SECURITY

3.1. Capsa Personnel. Capsa shall ensure that Capsa personnel engaged in the Processing of Personal Data on behalf of Distributor are informed of the confidential nature of the Personal Data and are subject to obligations of confidentiality that survive termination of such personnel's engagement with Capsa.

3.2. Security. Capsa will implement, maintain, and monitor a comprehensive information security program that contains appropriate administrative, physical, technical, and organizational safeguards to (a) ensure the confidentiality, integrity, and availability of Personal Data Capsa Processes on behalf of Distributor and (b) prevent loss of, destruction of, damage to, or unauthorized or unlawful Processing of Personal Data Capsa Processes on behalf of Distributor. The safeguards will be appropriate to the nature of the Personal Data, meet or exceed prevailing industry standards, and reasonably protect Personal Data Capsa Processes on behalf of Distributor. Capsa will comply with its information security program.

4. ASSISTANCE WITH DATA SUBJECT REQUESTS, DATA PROTECTION IMPACT ASSESSMENTS AND CONSULTATIONS WITH SUPERVISORY AUTHORITIES

4.1. Assistance Responding to Data Subject Requests. To the extent Distributor, in Distributor's use or receipt of the Services, does not have the ability to respond to requests from Data Subjects to exercise their rights under Data Protection Requirements, Capsa shall take reasonable steps to assist Distributor in fulfilling its obligations under Data Protection Requirements. If Capsa receives a request directly from a Data Subject, Capsa will inform the Data Subject that the request cannot be acted upon because the request has been sent to a Processor, and that such request must be redirected to the appropriate Controller.

4.2. Additional Assistance. Taking into account the nature of Processing and the information available to Capsa, Capsa will reasonably cooperate with Distributor, at Distributor's expense, to assist Distributor in ensuring compliance with its obligations to (a) securely Process Personal Data, (b) provide notification in the event of a Security Breach, (c) assess the impact of Processing activities on the protection of Personal Data and (d) consult with a Supervisory Authority or other regulatory body regarding the Processing of Personal Data when required by Data Protection Requirements.

5. SUBCONTRACTORS

5.1. General Authorization. Distributor generally authorizes the use of subprocessors to Process Personal Data on behalf of Distributor in connection with fulfilling Capsa's obligations under the Agreement and this DPA.

5.2. New Subprocessors. Capsa maintains a list of its current subprocessors online at www.capsahealthcare.com/legal/subprocessors_2021.pdf . When Capsa engages any new subprocessor to Process Personal Data on behalf of Distributor, Capsa will provide prior notice of the engagement by updating the list with the new subprocessor's name 30 days before the new subprocessor Processes any Personal Data on behalf of Distributor.

5.3. Capsa Obligations. Capsa will remain liable for the acts and omissions of its subprocessors to the same extent Capsa would be liable if performing the Services of each subprocessor directly under the terms of this DPA. Capsa will contractually impose data protection obligations on its subprocessors that are at least equivalent to those data protection obligations imposed on Capsa under this DPA.

6. CROSS-BORDER DATA TRANSFERS

6.1. European Personal Data Transfers. If Distributor Processes Personal Data about Data Subjects located in the European Economic Area, Switzerland, or the United Kingdom, Distributor and Capsa agree that the transfer or disclosure of such Personal Data to Capsa will be subject to (a) the protections in the Standard Contractual Clauses, or (b) another lawful cross-border transfer mechanism approved by the European Commission.

6.2. Standard Contractual Clauses. If the parties rely on the Standard Contractual Clauses in accordance with Section 6.1(a), the Standard Contractual Clauses will be deemed executed by the parties as of the Effective Date of the Agreement, and the following terms will apply: (a) Distributor will be referred to as the "data exporter" and Capsa will be referred to as the "data importer," with relevant name and address details from the Agreement being used accordingly, (b) details in Annex 1 to this DPA will be used to complete Appendix 1 of the Standard Contractual Clauses, (c) details in Annex 2 to this DPA will be used to complete Appendix 2 of the

Standard Contractual Clauses, and (d) if there is any conflict between this DPA or the Agreement and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail.

6.3. Other Personal Data Transfers. When Distributor transfers Personal Data about Data Subjects located in any other jurisdiction to Capsa, Distributor shall certify to and participate in a lawful cross-border transfer mechanism, where required.

7. SECURITY BREACH

7.1. Notification Obligations. In the event Capsa becomes aware of any Security Breach, Capsa will notify Distributor of the Security Breach without undue delay by sending an email to the email address associated with Distributor's account. It is Distributor's sole responsibility to maintain accurate contact information in connection with its account at all times.

8. TERM AND TERMINATION

8.1. Term of DPA. This DPA will remain in effect until, and automatically expire upon, the deletion or return of all Personal Data as described in Section 8.2.

8.2. Deletion or Return of Distributor Personal Data. Capsa shall delete or return Personal Data to Distributor after the end of the provision of Services under the Agreement and shall delete all existing copies thereof, except to the extent that (a) Capsa is required under Data Protection Requirements to keep a copy of the Personal Data or (b) the Controller otherwise authorizes Capsa's continued Processing of the Personal Data.

9. AUDITS

9.1. Audit Rights. No more than once per year, Distributor may engage a mutually-agreed upon third party to audit Capsa solely for the purpose of meeting Distributor's audit requirements pursuant to Article 28, Section 3(h) of the GDPR or other similar Data Protection Requirements. To request an audit, Distributor must submit a detailed audit plan at least four (4) weeks in advance of the proposed audit date describing the proposed scope, duration, and start date of the audit. Audit requests must be sent to dpo@capsahealthcare.com. The auditor must execute a written confidentiality agreement acceptable to Capsa before conducting the audit. The audit must be conducted during regular business hours, subject to Capsa's policies, and may not unreasonably interfere with Capsa's business activities. Any audits are at Distributor's sole cost and expense.

9.2. Separate Service. Any request for Capsa to assist with an audit is considered a separate service if such audit assistance requires the use of resources different from or in addition to those required by law. Distributor shall reimburse Capsa for any time spent for any such audit at mutually agreed-upon rates, taking into account the resources expended by Capsa. Distributor shall promptly provide Capsa with information regarding any non-compliance discovered during the course of an audit.

Annex 1

Scope of Processing

1. Subject Matter:

Capsa's provision of the Services under the Agreement and any Statement of Work.

2. Duration of Processing:

The term of the Agreement, plus the period from expiry of the term of the Agreement until Capsa has deleted or returned all Personal Data pursuant to this DPA.

3. Nature and Purpose of Processing:

Capsa will Process Personal Data on behalf of Distributor for the purpose of providing the Services in accordance with the Agreement and any Statement of Work.

4. Types of Personal Data may include:

For Kirby-Lester:

- Identifying data such as user and patient name, user ID, patient address, patient date of birth
- Special categories of information:
  - Data concerning health of patients (e.g., prescribed medication)
  - Biometric data of user

For N-Sight:

- Identifying data such as name, ID
- Location information, such as MAC address, of computers or devices
- User's departmental affiliation in Distributor's customer's organization

For Nexsys:

- Identifying data such as name, ID of users, medical providers, patients, pharmacists
- Location information of patients (e.g., assigned patient location)
- Patient gender
- Employment data of users (e.g., work email, phone number, role)
- Special categories of data:
  - Data concerning health of patients (e.g., admission information, allergy information, prescription data)
  - Biometric data of users

5. Categories of Data Subjects

For Kirby-Lester:

- Users
- Administrators
- Patients

For N-Sight:

- Users
- Administrators

For Nexsys:

- Users
- Administrators
- Physicians or other healthcare workers providing orders
- Patients
- Pharmacists

Annex 2

Description of Technical and Organizational Measures

This Annex describes the technical and organizational security measures implemented by Capsa in accordance with Clauses 4(d) and 5(c) of the Standard Contractual Clauses:

In addition to any technical and security measures described in the Security section of the DPA, Capsa implements the following measures:

- Capsa maintains an annual ISO27001 IT security certification;
- Capsa Products encrypt data in transit and at rest;
- Capsa employees receive regular training on data security; and
- Capsa employees agree to a comprehensive confidentiality/non-disclosure agreement at the time of employment.