BUSINESS ASSOCIATE AGREEMENT

Governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA),
as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act,
and implementing regulations at 45 C.F.R. Parts 160, 162, and 164

COVERED ENTITY: [COVERED ENTITY LEGAL NAME], a **[STATE AND ENTITY TYPE, e.g., Texas limited liability company]**, with its principal place of business at **[COVERED ENTITY ADDRESS, CITY, STATE, ZIP]** (hereinafter referred to as **"Covered Entity"** or **"CE"**).

BUSINESS ASSOCIATE: Texas Kaixingda Technology Development, LLC, a Texas limited liability company, doing business as *Sunny & Saima Assisted Living Homes*, with its principal place of business at 1109 Holly Street, La Marque, Texas 77568 (hereinafter referred to as **"Business Associate"** or **"BA"**).

Effective Date: [EFFECTIVE DATE]

TABLE OF CONTENTS

Section 1. Recitals

WHEREAS, Covered Entity is a covered entity as that term is defined under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (**"HIPAA"**), as amended by the Health Information Technology for Economic and Clinical Health Act, enacted as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Public Law 111-5 (**"HITECH Act"**), and the implementing regulations promulgated thereunder, including without limitation the Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Parts 160 and 164, Subparts A and E (the **"Privacy Rule"**), the Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. Parts 160 and 164, Subparts A and C (the **"Security Rule"**), and the Notification in the Case of Breach of Unsecured Protected Health Information, 45 C.F.R. Parts 160 and 164, Subpart D (the **"Breach Notification Rule"**), all as may be amended from time to time (collectively, **"HIPAA Rules"**);

WHEREAS, Business Associate provides certain services to Covered Entity pursuant to a separate services agreement or engagement (the **"Services Agreement"**), which services include the provision of a software-as-a-service (SaaS) care delivery and compliance platform that facilitates the creation, receipt, maintenance, and/or transmission of Protected Health Information (as defined herein) on behalf of Covered Entity;

WHEREAS, in connection with such services, Business Associate may receive, create, maintain, transmit, use, or disclose Protected Health Information belonging to patients,

residents, and individuals served by Covered Entity, thereby constituting Business Associate as a "business associate" of Covered Entity within the meaning of 45 C.F.R. § 160.103;

WHEREAS, HIPAA, the HITECH Act, and 45 C.F.R. Parts 160, 162, and 164 require Covered Entity to enter into a written Business Associate Agreement with Business Associate as a condition of permitting Business Associate to create, receive, maintain, or transmit Protected Health Information on behalf of Covered Entity;

WHEREAS, both parties intend to protect the privacy and security of Protected Health Information in compliance with all applicable federal and state laws, regulations, and guidance;

NOW, THEREFORE, in consideration of the mutual covenants and agreements set forth herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

Section 2. Definitions

Capitalized terms not otherwise defined herein shall have the same meanings as set forth in the HIPAA Rules, including 45 C.F.R. §§ 160.103 and 164.304. In the event of any conflict between this Agreement and the HIPAA Rules, the HIPAA Rules shall control. The following definitions shall apply for purposes of this Agreement:

2.1 "Agreement" means this Business Associate Agreement, including any exhibits, schedules, or amendments attached hereto or incorporated herein by reference.

2.2 "Breach" means the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under the Privacy Rule that compromises the security or privacy of such information, as defined at 45 C.F.R. § 164.402. Breach shall not include: (a) any unintentional acquisition, access, or use of Protected Health Information by a workforce member or person acting under the authority of Business Associate or Covered Entity, if such acquisition, access, or use was made in good faith and within the scope of

authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule; (b) any inadvertent disclosure by a person authorized to access Protected Health Information to another person authorized to access Protected Health Information, provided that such information is not further used or disclosed in a manner not permitted under the Privacy Rule; or (c) a disclosure of Protected Health Information where Covered Entity or Business Associate has a good-faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2.3 "Business Associate" shall generally have the same meaning as the term "business associate" at 45 C.F.R. § 160.103, and in reference to the party to this Agreement, shall mean Texas Kaixingda Technology Development, LLC dba Sunny & Saima Assisted Living Homes.

2.4 "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 C.F.R. § 160.103, and in reference to the party to this Agreement, shall mean **[COVERED ENTITY LEGAL NAME]**.

2.5 "Electronic Protected Health Information" or "ePHI" means Protected Health Information that is transmitted by or maintained in electronic media, as set forth at 45 C.F.R. § 160.103.

2.6 "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, as amended from time to time, and all regulations promulgated thereunder, including but not limited to those set forth at 45 C.F.R. Parts 160, 162, and 164.

2.7 "HITECH Act" means the Health Information Technology for Economic and Clinical Health Act, enacted as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Public Law 111-5, as amended, and any applicable regulations, guidance, and rules promulgated thereunder.

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

2.9 "Privacy Rule" means the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and E, as currently in effect or as amended.

2.10 "Protected Health Information" or "PHI" shall have the same meaning as the term "protected health information" in 45 C.F.R. § 160.103, limited to information created, received, maintained, or transmitted by Business Associate from or on behalf of Covered Entity. For the avoidance of doubt, PHI includes Electronic Protected Health Information (ePHI).

2.11 "Required by Law" shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.103.

2.12 "Secretary" means the Secretary of the U.S. Department of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated, as set forth at 45 C.F.R. § 160.103.

2.13 "Security Incident" shall have the same meaning as the term "security incident" in 45 C.F.R. § 164.304, meaning the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system that maintains Electronic Protected Health Information.

2.14 "Security Rule" means the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and C, as currently in effect or as amended.

2.15 "Services Agreement" means any separately executed agreement, statement of work, order form, or other contractual instrument between Covered Entity and Business Associate pursuant to which Business Associate provides services to Covered Entity involving the creation, receipt, maintenance, or transmission of Protected Health Information.

2.16 "Subcontractor" shall have the same meaning as the term "subcontractor" in 45 C.F.R. § 160.103, meaning a person or entity to whom a business associate delegates a function,

activity, or service, other than in the capacity of a member of the workforce of such business associate.

2.17 "Unsecured PHI" means Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance issued pursuant to 45 C.F.R. § 164.402.

Section 3. Obligations and Activities of Business Associate

3.1 Permitted Uses and Disclosures

Business Associate shall use or disclose PHI only as expressly authorized herein or as Required by Law. Permitted uses and disclosures include the following:

1. **Care Delivery Platform Operations.** Business Associate may use and disclose PHI as necessary to provide, operate, and support the SaaS care delivery and compliance platform, including facilitating care coordination, scheduling, documentation of care activities, medication management records, and related functions performed on behalf of Covered Entity.
2. **Compliance Reporting.** Business Associate may use and disclose PHI as necessary to generate compliance reports, regulatory submissions, and quality assurance documentation as directed by and for the benefit of Covered Entity.
3. **Authorized Health Care Operations.** Business Associate may use PHI for health care operations of Covered Entity as defined in 45 C.F.R. § 164.501, including quality assessment and improvement activities, to the extent such use is authorized under this Agreement and permitted by the Privacy Rule.
4. **Required by Law.** Business Associate may disclose PHI to the extent Required by Law, provided that Business Associate shall notify Covered Entity of such

requirement prior to disclosure (to the extent practicable and not prohibited by law) and shall cooperate with Covered Entity with respect to any protective order or similar relief.

5. **Proper Management and Administration.** Business Associate may use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, as further described in Section 9 of this Agreement.

3.2 Prohibition on Unauthorized Use or Disclosure

Business Associate shall not use or disclose PHI other than as permitted or required by this Agreement or as Required by Law. Business Associate shall not use or disclose PHI in any manner that would violate the Privacy Rule if done by Covered Entity. Business Associate shall not sell PHI, use PHI for marketing purposes, or use or disclose PHI in a manner that constitutes a prohibited sale of PHI under 45 C.F.R. § 164.502(a)(5). Business Associate shall not use PHI for research purposes without prior written authorization from Covered Entity and, where required, appropriate individual authorization or a waiver thereof. Business Associate shall not disclose PHI to any third party not expressly authorized under this Agreement without the prior written consent of Covered Entity.

3.3 Safeguards

Business Associate shall implement and maintain appropriate administrative, physical, and technical safeguards to prevent the use or disclosure of PHI other than as provided for by this Agreement, and to reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI, consistent with the requirements of 45 C.F.R. §§ 164.308, 164.310, and 164.312. Without limiting the foregoing, Business Associate shall, at a minimum, implement and maintain the following safeguards:

6. **Encryption in Transit.** All ePHI transmitted across public or open networks shall be encrypted using Transport Layer Security (TLS) version 1.2 or higher, or a comparable or stronger standard approved in writing by Covered Entity.

7. **Encryption at Rest.** All ePHI stored or maintained in any information system, database, server, device, or storage medium shall be encrypted using the Advanced Encryption Standard (AES) with a key length of not less than 256 bits (AES-256), or a comparable or stronger standard approved in writing by Covered Entity.
8. **Role-Based Access Control (RBAC).** Business Associate shall implement and enforce a role-based access control system that limits access to ePHI to workforce members and authorized users whose job functions require such access. Access rights shall be assigned based on the principle of least privilege. Business Associate shall conduct periodic access reviews not less than semi-annually and shall promptly revoke access upon termination of employment or change of role.
9. **Multi-Factor Authentication (MFA).** Business Associate shall require multi-factor authentication for all personnel, contractors, agents, and subcontractors who access, or are capable of accessing, any system containing ePHI. MFA shall be implemented in accordance with current National Institute of Standards and Technology (NIST) guidelines and shall not be subject to exception without documented written justification and Covered Entity's prior written approval.
10. **Audit Logging.** Business Associate shall implement and maintain comprehensive audit logging of all access to, and all modifications, additions, or deletions of, ePHI. Audit logs shall be retained for a minimum of six (6) years, shall be protected from unauthorized access, deletion, or alteration, and shall be made available to Covered Entity upon written request.
11. **Regular Risk Assessments.** Business Associate shall conduct, document, and review Security Risk Assessments of its electronic information systems containing or transmitting ePHI no less frequently than annually, or promptly following any significant environmental or operational change, in accordance with 45 C.F.R. § 164.308(a)(1). The results of each risk assessment and Business Associate's risk management plan shall be made available to Covered Entity upon written request.

12. **Workforce Training.** Business Associate shall train all members of its workforce on the HIPAA Privacy Rule, Security Rule, and this Agreement's requirements, upon hire and not less than annually thereafter.
13. **Contingency Planning.** Business Associate shall maintain a data backup plan, disaster recovery plan, and emergency mode operation plan for all systems containing ePHI, consistent with 45 C.F.R. § 164.308(a)(7).

3.4 Reporting of Security Incidents and Breaches

3.4.1 Breach Notification. Business Associate shall notify Covered Entity in writing without unreasonable delay, and in no event later than five (5) business days after Business Associate's discovery of a Breach of Unsecured PHI, as defined at 45 C.F.R. § 164.402. For purposes of this provision, a Breach shall be deemed "discovered" as of the first day on which such Breach is known to Business Associate, or by exercising reasonable diligence would have been known to Business Associate. Such notification shall include, to the extent possible at the time of notification:

14. The identification of each Individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used, or disclosed during the Breach;
15. A brief description of what happened, including the date of the Breach and the date of discovery of the Breach, if known;
16. A description of the types of Unsecured PHI involved in the Breach (e.g., whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
17. Any steps Individuals should take to protect themselves from potential harm resulting from the Breach;
18. 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

19. Contact information for Business Associate (or the Services Agreement under which the Breach occurred).

If not all required information is available at the time of initial notification, Business Associate shall provide the available information and shall supplement such notification as additional information becomes available, without unreasonable delay.

3.4.2 Security Incident Reporting. Business Associate shall report to Covered Entity any Security Incident that does not rise to the level of a Breach of Unsecured PHI within seventy-two (72) hours of discovery. Such report shall describe: (a) the nature of the Security Incident; (b) the ePHI involved, if any; (c) corrective actions taken or planned; and (d) the name and contact information of a Business Associate representative responsible for handling the incident.

3.4.3 Notice of Unsuccessful Security Incidents. The parties acknowledge that attempted but unsuccessful Security Incidents (including, without limitation, pings, port scans, denial-of-service attacks, and malware activity that do not result in unauthorized access, use, disclosure, modification, or destruction of ePHI) occur on a routine basis and that written notice and reports of each such unsuccessful incident are not required under this Agreement. Business Associate shall report such patterns or trends to Covered Entity upon request.

3.5 Subcontractors

Business Associate shall not disclose PHI to any Subcontractor without ensuring, in accordance with 45 C.F.R. § 164.308(b)(2) and § 164.502(e)(1)(ii), that the Subcontractor agrees in writing, through a business associate agreement, to the same restrictions, conditions, and requirements that apply to Business Associate under this Agreement with respect to PHI. Business Associate shall be fully responsible and liable to Covered Entity for the acts and omissions of its Subcontractors as if Business Associate had directly committed such acts or omissions. Business Associate shall monitor Subcontractor compliance on an ongoing basis. If Business Associate discovers that a Subcontractor has materially breached any provision of its subcontractor business associate agreement, Business Associate shall promptly notify Covered Entity and take reasonable steps to cure the breach or end the

violation, including, if necessary, terminating the subcontractor arrangement. Business Associate shall maintain a current list of Subcontractors that access, receive, maintain, or transmit PHI on behalf of Business Associate and shall make such list available to Covered Entity upon written request within ten (10) business days of such request.

3.6 Access to PHI; Individual Rights

Business Associate shall, within ten (10) business days of a written request by Covered Entity, take such action with respect to PHI in Business Associate's possession as is necessary to enable Covered Entity to fulfill its obligations to Individuals under the Privacy Rule, including:

20. **Right of Access.** Provide access to PHI in a designated record set maintained by Business Associate to Covered Entity or, as directed by Covered Entity, to an Individual, as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.524;
21. **Amendment.** Make any amendment(s) to PHI in a designated record set as directed by or agreed to by Covered Entity pursuant to 45 C.F.R. § 164.526, or take other measures as necessary to satisfy Covered Entity's obligations thereunder; and
22. **Accounting of Disclosures.** Maintain and 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 C.F.R. § 164.528, and provide such information to Covered Entity upon written request.

3.7 Availability of Books and Records to HHS

Business Associate shall make its internal practices, books, records, policies, procedures, and other documentation relating to the use and disclosure of PHI available to the Secretary for purposes of determining Covered Entity's compliance with the HIPAA Rules, in accordance with 45 C.F.R. § 164.504(e)(2)(ii)(H). Business Associate shall promptly notify Covered Entity of any such access or request for access by the Secretary.

3.8 Minimum Necessary

Business Associate shall, in accordance with 45 C.F.R. § 164.514(d), make reasonable efforts to use, disclose, and request only the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure, or request. Business Associate shall implement policies and procedures to limit its workforce's access to PHI to the minimum necessary to perform their functions.

3.9 De-identification

Business Associate shall not de-identify PHI, or cause PHI to be de-identified, except with the prior written approval of Covered Entity and in strict compliance with the de-identification standards set forth at 45 C.F.R. § 164.514(a)–(c). Any de-identification methodology employed shall be documented and provided to Covered Entity upon request. De-identified information that meets the standards of 45 C.F.R. § 164.514(b) shall not be considered PHI subject to this Agreement.

3.10 Data Aggregation

Business Associate may perform data aggregation services relating to the health care operations of Covered Entity only with the prior written approval of Covered Entity, in accordance with 45 C.F.R. § 164.504(e)(2)(i)(B). Any data aggregation activities shall be described with particularity in written authorization from Covered Entity and shall be performed in a manner consistent with the Privacy Rule and the terms of this Agreement.

Section 4. Obligations of Covered Entity

4.1 Notice of Privacy Practices

Covered Entity shall notify Business Associate of any limitations in Covered Entity's Notice of Privacy Practices established in accordance with 45 C.F.R. § 164.520, to the extent that such limitations may affect Business Associate's use or disclosure of PHI under this

Agreement. Covered Entity shall provide Business Associate with a current copy of its Notice of Privacy Practices and shall promptly update Business Associate of any changes thereto that may affect Business Associate's permitted uses or disclosures of PHI.

4.2 Permission Changes

Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's permitted uses or disclosures under this Agreement. Such notification shall be provided in writing and within a reasonable time before the effective date of such changes, to the extent practicable.

4.3 Restrictions on Use and Disclosure

Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI. Such notification shall be provided in writing promptly after Covered Entity agrees to or becomes aware of such restriction.

4.4 Lawful Requests and Instructions

Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Covered Entity, except that Covered Entity may authorize Business Associate to use or disclose PHI for data aggregation and management and administration purposes, as described in Section 9 of this Agreement, to the extent permitted by applicable law.

4.5 Safeguards

Covered Entity shall implement appropriate administrative, physical, and technical safeguards to protect PHI it shares with Business Associate, including ensuring the security of transmissions of PHI to Business Associate.

Section 5. Term and Termination

5.1 Term

This Agreement shall be effective as of the Effective Date first written above and shall remain in full force and effect coterminous with the term of the underlying Services Agreement, unless earlier terminated in accordance with the provisions hereof. This Agreement shall automatically renew upon any renewal of the Services Agreement unless a party provides written notice of its intent not to renew at least thirty (30) days prior to the expiration of the then-current term.

5.2 Termination for Cause

Covered Entity may terminate this Agreement and the Services Agreement, in whole or in part, upon written notice to Business Associate if Business Associate materially breaches any provision of this Agreement, including any obligation imposed by the HIPAA Rules. Prior to termination for cause, Covered Entity shall provide Business Associate with written notice of the breach and a reasonable opportunity to cure, not to exceed thirty (30) calendar days from the date of such notice, provided that such cure is feasible. If Business Associate fails to cure the breach within the applicable cure period, or if Business Associate notifies Covered Entity that it does not intend to cure the breach, or if cure is not feasible in Covered Entity's reasonable determination, Covered Entity may terminate this Agreement and the Services Agreement immediately upon written notice. Nothing in this subsection shall limit Covered Entity's right to seek injunctive or other equitable relief in a court of competent jurisdiction to prevent harm from continuing violations.

5.3 Automatic Termination

This Agreement shall terminate automatically, without further action by either party, upon the expiration or termination of the Services Agreement for any reason. Upon such automatic termination, the obligations of this Agreement that by their nature survive termination, including those set forth in Section 5.4 and Section 5.5, shall remain in full force and effect.

5.4 Effect of Termination; Return and Destruction of PHI

5.4.1 Return or Destruction. Upon termination or expiration of this Agreement for any reason, Business Associate shall, within forty-five (45) calendar days of the effective date of termination or expiration, return to Covered Entity or destroy all PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, that Business Associate still maintains in any form, including any PHI in the possession of Subcontractors. Business Associate shall certify in writing to Covered Entity that all PHI has been returned or destroyed, as applicable, within the same forty-five (45) day period. Business Associate shall not retain any copies of PHI following return or destruction except as required by law.

5.4.2 Infeasibility of Return or Destruction. To the extent that Business Associate determines that return or destruction of any PHI is not feasible (including PHI in the possession of a Subcontractor), Business Associate shall: (a) provide Covered Entity with a written certification identifying the PHI retained and the specific reasons why return or destruction is not feasible; (b) extend the protections of this Agreement to such retained PHI for as long as Business Associate retains such PHI; (c) limit further uses or disclosures of such retained PHI to those purposes that make the return or destruction of PHI infeasible; and (d) return or destroy such retained PHI when it is no longer required to be retained by law or regulation, and provide written certification of such return or destruction to Covered Entity.

5.5 Survival

The provisions of Section 2 (Definitions), Section 5.4 (Effect of Termination), Section 5.5 (Survival), Section 6 (Breach Notification Procedures), Section 10 (Indemnification), and Section 11 (Miscellaneous) shall survive termination or expiration of this Agreement for any reason. Obligations that accrued prior to the date of termination shall not be extinguished by termination of this Agreement.

Section 6. Breach Notification Procedures

6.1 Discovery of Breach

Upon discovery of a Breach of Unsecured PHI, Business Associate shall take immediate steps to contain and mitigate the Breach and shall conduct a thorough investigation to determine the scope, cause, and nature of the Breach. Business Associate shall document its investigation findings and maintain such documentation for a minimum of six (6) years from the date of the Breach.

6.2 Notification to Covered Entity

Business Associate shall notify Covered Entity of a Breach of Unsecured PHI in writing without unreasonable delay, and in no event later than five (5) business days after Business Associate's discovery of such Breach, as required by 45 C.F.R. § 164.410. Such written notification shall include, to the extent available at the time of notification, all of the following:

23. The identity of each Individual whose Unsecured PHI was, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of the Breach;
24. A brief description of what happened, including the date of the Breach, if known, and the date of discovery;
25. A description of the types of Unsecured PHI involved (e.g., name, social security number, date of birth, address, diagnosis, treatment information, financial information, or other categories);
26. Any steps Individuals should take to protect themselves from potential harm resulting from the Breach;
27. A description of what Business Associate is doing to investigate the Breach, mitigate harm to affected Individuals, and protect against recurrence; and
28. Contact information for the Business Associate representative responsible for breach notification, including name, telephone number, and email address.

6.3 Covered Entity Notification Responsibilities

Following receipt of Business Associate's breach notification, Covered Entity shall assess whether the Breach triggers its own obligations to notify affected Individuals, the Secretary, and, if applicable, prominent media outlets, in accordance with 45 C.F.R. §§ 164.400 through 164.414. Business Associate shall cooperate fully with Covered Entity in conducting such assessment and in complying with Covered Entity's notification obligations.

6.4 Presumption of Breach

Any unauthorized acquisition, access, use, or disclosure of PHI shall be presumed to be a Breach unless Business Associate demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the factors enumerated at 45 C.F.R. § 164.402(2). Such risk assessment shall be documented in writing and shall be provided to Covered Entity upon written request.

6.5 Cooperation and Mitigation

Business Associate shall cooperate fully with Covered Entity in any investigation of a Breach, including providing Covered Entity with prompt access to Business Associate's relevant systems, logs, records, policies, and workforce members. Business Associate shall take all reasonable steps to mitigate, to the extent practicable, any harmful effect of a Breach that is known to Business Associate.

6.6 Costs of Breach

In the event that a Breach results from Business Associate's failure to comply with its obligations under this Agreement, applicable law, or reasonable industry security standards, Business Associate shall bear all reasonable and documented costs associated with such Breach, including but not limited to: (a) the costs of notification to affected Individuals; (b) the costs of notification to the Secretary and any applicable media outlets; (c) the costs of providing credit monitoring or identity theft protection services to affected Individuals; (d) reasonable legal fees and expenses; and (e) regulatory fines and penalties assessed against Covered Entity as a direct result of Business Associate's failure. The foregoing shall be in

addition to, and not in lieu of, any indemnification obligations set forth in Section 10 of this Agreement.

Section 7. Security Requirements

7.1 Incorporation of HIPAA Security Rule

Business Associate hereby formally incorporates and agrees to comply with the full requirements of the HIPAA Security Rule, including all administrative safeguard standards (45 C.F.R. § 164.308), physical safeguard standards (45 C.F.R. § 164.310), and technical safeguard standards (45 C.F.R. § 164.312), as applicable to business associates, and as amended from time to time. Compliance with the Security Rule shall be interpreted as a minimum standard; Business Associate shall implement controls exceeding this standard where the nature of the ePHI maintained or the risk environment so warrants.

7.2 Administrative Safeguards (45 C.F.R. § 164.308)

Business Associate shall implement the following administrative safeguards, at a minimum:

29. A security management process including risk analysis, risk management, sanction policy, and information system activity review;
30. Assigned security responsibility designating an individual responsible for the development and implementation of the Business Associate's security policies and procedures;
31. Workforce security controls including authorization and supervision, workforce clearance procedures, and termination procedures;
32. Information access management including isolating health care clearinghouse functions (if applicable), access authorization, and access establishment and modification procedures;
33. Security awareness and training programs for all workforce members;

34. Security incident procedures for identifying, responding to, reporting, and mitigating security incidents; and
35. A contingency plan including data backup, disaster recovery, emergency mode operations, testing, and revision procedures.

7.3 Physical Safeguards (45 C.F.R. § 164.310)

Business Associate shall implement physical safeguards including facility access controls, workstation use and security policies, and device and media controls governing the receipt, removal, and disposal of hardware and electronic media containing ePHI.

7.4 Technical Safeguards (45 C.F.R. § 164.312)

Business Associate shall implement and maintain the following technical safeguards and controls:

36. **Encryption in Transit:** All transmission of ePHI shall be protected using TLS version 1.2 or higher. Older protocol versions (SSLv3, TLS 1.0, TLS 1.1) shall be disabled on all systems used to transmit ePHI;
37. **Encryption at Rest:** All ePHI maintained on any server, workstation, portable device, backup media, or cloud storage shall be encrypted using AES-256 or stronger. Encryption keys shall be managed in accordance with current NIST guidelines;
38. **Role-Based Access Control (RBAC):** Access to ePHI shall be granted based solely on role and minimum necessary need. Privileged access shall be separately tracked and reviewed;
39. **Multi-Factor Authentication (MFA):** All accounts capable of accessing systems containing ePHI shall require MFA, without exception, including service accounts where technically feasible;
40. **Comprehensive Audit Logging:** Business Associate shall maintain audit logs capturing user access, authentication events, data access and modification events,

and administrative actions affecting systems containing ePHI. Logs shall be immutable, protected from alteration, and retained for a minimum of six (6) years; and

41. **Automatic Logoff:** Systems accessing ePHI shall implement automatic logoff after a reasonable period of inactivity, consistent with 45 C.F.R. § 164.312(a)(2)(iii).

7.5 Written Policies and Procedures

Business Associate shall maintain written security policies and procedures that implement the safeguards required under this Section and the HIPAA Security Rule. Such policies and procedures shall be reviewed and updated at least annually, or more frequently as warranted by changes in the environment or operations of Business Associate. Business Associate shall retain all security policies, procedures, and records of activity for a minimum of six (6) years from the date of creation or the date last in effect, whichever is later.

7.6 Annual Security Risk Assessment

Business Associate shall conduct, at a minimum, an annual Security Risk Assessment in accordance with 45 C.F.R. § 164.308(a)(1). Such assessments shall: (a) identify foreseeable threats and vulnerabilities to the confidentiality, integrity, and availability of ePHI; (b) assess the likelihood and impact of such threats; (c) implement security measures sufficient to reduce identified risks to a reasonable and appropriate level; and (d) produce a written risk management plan with assigned responsibilities and remediation timelines. Business Associate shall provide Covered Entity with a summary of its annual Security Risk Assessment results and risk management plan upon Covered Entity's written request.

7.7 Security Attestation

Business Associate shall, upon written request by Covered Entity (not more than once per calendar year absent a Security Incident or Breach), provide Covered Entity with a written attestation, signed by a duly authorized officer or security official of Business Associate, certifying Business Associate's compliance with the security requirements of this Agreement

and the HIPAA Security Rule. Such attestation shall be delivered within thirty (30) calendar days of Business Associate's receipt of Covered Entity's written request.

Section 8. Subcontractor Requirements

8.1 Subcontractor Business Associate Agreements

Business Associate shall not disclose PHI to any Subcontractor, agent, or third party unless Business Associate has first obtained a written business associate agreement from such Subcontractor that imposes on the Subcontractor the same restrictions, conditions, and requirements that this Agreement imposes on Business Associate with respect to PHI, in accordance with 45 C.F.R. § 164.308(b)(2) and § 164.502(e)(1)(ii). Such subcontractor business associate agreement shall: (a) expressly prohibit the Subcontractor from further disclosing PHI except as permitted under the agreement; (b) require the Subcontractor to implement the administrative, physical, and technical safeguards required of Business Associate under this Agreement; (c) require the Subcontractor to report Security Incidents and Breaches directly to Business Associate, who shall in turn notify Covered Entity in accordance with Section 6 of this Agreement; and (d) require the Subcontractor to comply with all applicable provisions of the HIPAA Rules.

8.2 Monitoring Subcontractor Compliance

Business Associate shall actively monitor and assess the compliance of each Subcontractor with the Subcontractor's business associate agreement on an ongoing basis. Such monitoring shall include, at a minimum: (a) initial due diligence prior to engagement; (b) annual review of the Subcontractor's security posture, including review of the Subcontractor's most recent security assessment, audit reports, or certifications (such as SOC 2 Type II or equivalent); and (c) prompt investigation of any reported or suspected non-compliance.

8.3 Termination of Subcontractor Relationship

If Business Associate discovers that a Subcontractor has materially breached its business associate agreement, Business Associate shall promptly: (a) notify Covered Entity in writing of the material breach within five (5) business days of discovery; (b) take reasonable steps to cure the breach or end the violation; and (c) if steps to cure the breach are unsuccessful within a reasonable period, terminate the subcontractor relationship and ensure the secure return or destruction of all PHI in the Subcontractor's possession. Business Associate shall document all such actions and provide Covered Entity with a written summary of the steps taken upon request.

8.4 Business Associate Liability for Subcontractors

Business Associate shall remain fully liable to Covered Entity for any acts or omissions of its Subcontractors that constitute a violation of Business Associate's obligations under this Agreement, to the same extent as if Business Associate had directly committed such acts or omissions. The existence of a subcontractor business associate agreement shall not limit Business Associate's liability to Covered Entity under this Agreement or applicable law.

8.5 Subcontractor Disclosure List

Business Associate shall maintain a current, written list of all Subcontractors and agents who access, receive, maintain, or transmit PHI on behalf of Business Associate in connection with the Services Agreement. Such list shall include, for each Subcontractor: the legal name; a brief description of the function performed; and confirmation that a current business associate agreement is in place. Business Associate shall make this list available to Covered Entity upon written request within ten (10) business days of receipt of such request.

Section 9. Permitted Uses by Business Associate

Except as otherwise limited in this Agreement, Business Associate may use PHI for the proper management and administration of Business Associate, or to carry out the legal

responsibilities of Business Associate, in accordance with 45 C.F.R. § 164.504(e)(4), subject to the following conditions:

9.1 Management and Administration

Business Associate may use PHI as necessary for the internal management and administration of Business Associate's operations, including but not limited to quality assurance, compliance monitoring, employee training, and business continuity activities. Such use shall be limited to the minimum PHI necessary and shall be subject to all safeguards required under this Agreement.

9.2 Legal Responsibilities

Business Associate may disclose PHI as necessary to carry out the legal responsibilities of Business Associate, provided that: (a) the disclosure is Required by Law; or (b) Business Associate obtains reasonable assurances from the recipient that: (i) the information will be held confidentially and used or further disclosed only as Required by Law or for the purpose for which it was disclosed; and (ii) the recipient will notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached. Business Associate shall promptly notify Covered Entity of any such disclosure.

9.3 Data Aggregation

Business Associate may perform data aggregation services relating to the health care operations of Covered Entity only as expressly authorized in advance and in writing by Covered Entity, as provided in Section 3.10 of this Agreement. Business Associate shall not aggregate PHI of Covered Entity with PHI of any other covered entity without the separate prior written consent of Covered Entity.

9.4 De-identification

Business Associate may de-identify PHI pursuant to 45 C.F.R. § 164.514 only as expressly authorized in advance and in writing by Covered Entity, as provided in Section 3.9 of this Agreement. Information de-identified in accordance with such authorization and the

standards of 45 C.F.R. § 164.514 shall no longer constitute PHI subject to the restrictions of this Agreement.

Section 10. Indemnification

10.1 Indemnification by Business Associate

Business Associate shall indemnify, defend, and hold harmless Covered Entity, and each of its members, managers, officers, directors, employees, agents, successors, and assigns (each an **"Indemnified Party"**), from and against any and all claims, actions, suits, proceedings, losses, liabilities, damages, fines, penalties, costs, and expenses (including reasonable attorneys' fees and court costs) (collectively, **"Losses"**) arising out of or relating to:

42. Any actual or alleged breach by Business Associate of this Agreement, including any breach of its obligations under the HIPAA Rules;
43. Any actual or alleged violation by Business Associate or any of its Subcontractors of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule, or the Breach Notification Rule;
44. Any unauthorized access to, use, disclosure, acquisition, or modification of PHI by Business Associate, its workforce members, agents, or Subcontractors;
45. Any Breach of Unsecured PHI caused by or attributable to Business Associate's acts or omissions; or
46. Any negligence, willful misconduct, or fraud of Business Associate, its workforce members, agents, or Subcontractors in connection with the performance of this Agreement.

10.2 Indemnification Procedure

An Indemnified Party seeking indemnification under this Section shall: (a) promptly notify Business Associate in writing of the claim or proceeding for which indemnification is sought;

(b) grant Business Associate the right to control the defense and settlement of such claim, provided that Covered Entity shall have the right to participate in the defense at its own expense and to approve any settlement that imposes any obligation or restriction on Covered Entity; and (c) provide reasonable cooperation to Business Associate in connection with such defense, at Business Associate's reasonable expense. Business Associate's obligation to indemnify shall not be reduced by any failure to provide prompt notice unless Business Associate is materially prejudiced by such delay.

10.3 Insurance

Business Associate shall, throughout the term of this Agreement and for a period of not less than three (3) years following termination, maintain at its own expense adequate insurance coverage, including: (a) commercial general liability insurance with limits of not less than **[MINIMUM COVERAGE AMOUNT, e.g., $1,000,000 per occurrence / $2,000,000 aggregate]**; and (b) cyber liability and data breach insurance with limits of not less than **[MINIMUM COVERAGE AMOUNT, e.g., $2,000,000 per occurrence]**. Upon written request, Business Associate shall provide Covered Entity with certificates of insurance evidencing such coverage.

Section 11. Miscellaneous Provisions

11.1 Amendment

This Agreement may not be amended, modified, or supplemented except by a written instrument duly signed by authorized representatives of both parties. Notwithstanding the foregoing, the parties agree to amend this Agreement as necessary to comply with the requirements of HIPAA, the HITECH Act, and any regulations or guidance promulgated thereunder, as amended from time to time, and to comply with any applicable state law requirements relating to the privacy and security of PHI. In the event of a conflict between this Agreement and any future regulatory requirement, the parties agree to negotiate in good faith to execute a written amendment within sixty (60) calendar days of the effective date of

such regulatory requirement, or such shorter period as may be required by the applicable regulation or guidance.

11.2 Interpretation

This Agreement shall be construed and interpreted to give maximum effect to the parties' intent to comply with all applicable requirements of HIPAA, the HITECH Act, and the HIPAA Rules, as currently in effect or as amended. Any ambiguity in this Agreement shall be resolved in a manner that effectuates such compliance. The parties acknowledge that the HIPAA Rules, as they may be amended from time to time, are incorporated herein by reference and shall be deemed part of this Agreement to the extent applicable. The headings in this Agreement are for reference only and shall not affect its interpretation.

11.3 No Third-Party Beneficiaries

This Agreement is entered into solely for the benefit of the parties hereto and their respective successors and permitted assigns. Nothing in this Agreement, express or implied, is intended to confer upon any other person or entity (including Individuals whose PHI is subject to this Agreement) any rights, remedies, obligations, or liabilities of any nature, except to the extent expressly provided herein or required by applicable law.

11.4 Governing Law

This Agreement shall be governed by and construed in accordance with the laws of the State of Texas, without regard to its conflict of laws principles. The parties acknowledge and agree that the requirements of federal law, including HIPAA, the HITECH Act, and the HIPAA Rules, shall supersede any conflicting provisions of state law to the extent required by applicable law. Any dispute arising out of or relating to this Agreement shall be resolved in a court of competent jurisdiction located in Galveston County, Texas, and the parties hereby consent to the personal jurisdiction of such courts.

11.5 Entire Agreement

This Agreement, together with the Services Agreement (which is incorporated herein by reference solely with respect to its description of the services giving rise to Business Associate's access to PHI), constitutes the entire agreement between the parties with respect to the subject matter hereof — namely, the privacy, security, and permitted use and disclosure of PHI. This Agreement supersedes all prior and contemporaneous oral and written representations, negotiations, statements, warranties, and understandings of the parties with respect to such subject matter. In the event of a conflict between this Agreement and the Services Agreement with respect to the handling of PHI, this Agreement shall control.

11.6 Severability

If any provision of this Agreement is found by a court of competent jurisdiction to be invalid, illegal, or unenforceable under applicable law, such provision shall be modified to the minimum extent necessary to make it valid, legal, and enforceable. If such modification is not possible, the relevant provision shall be deemed deleted. Such invalidity, illegality, or unenforceability shall not affect the validity, legality, or enforceability of any other provision of this Agreement, which shall remain in full force and effect.

11.7 Waiver

No failure or delay by either party in exercising any right, power, or privilege under this Agreement shall operate as a waiver thereof, nor shall any single or partial exercise of any right, power, or privilege preclude any other or further exercise thereof or the exercise of any other right, power, or privilege. No waiver of any provision of this Agreement shall be effective unless made in writing and signed by the waiving party. Any waiver shall be limited to the specific instance and purpose for which it is given.

11.8 Counterparts and Electronic Signatures

This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, and all of which together shall constitute one and the same instrument. Electronic signatures, including signatures transmitted by PDF, DocuSign, or other electronic signature platform compliant with the Electronic Signatures in Global and National

Commerce Act (E-SIGN Act), 15 U.S.C. § 7001 et seq., and the Texas Uniform Electronic Transactions Act, Tex. Bus. & Com. Code § 322.001 et seq., shall be deemed valid and binding to the same extent as original ink signatures. Executed copies delivered electronically shall have the same force and effect as originals.

11.9 Notices

All notices, requests, demands, consents, and other communications required or permitted under this Agreement shall be in writing and shall be deemed duly given when: (a) delivered personally; (b) sent by nationally recognized overnight courier (with written confirmation of receipt); (c) sent by certified or registered mail, return receipt requested, postage prepaid; or (d) sent by encrypted electronic mail with confirmation of receipt by the recipient (provided that a copy is simultaneously delivered by one of the methods described in (a)–(c) above). Notices shall be addressed as follows:

If to Covered Entity:	If to Business Associate:
[COVERED ENTITY LEGAL NAME] **[STREET ADDRESS]** **[CITY, STATE, ZIP]** Attention: **[COVERED ENTITY CONTACT NAME AND TITLE]** Email: **[COVERED ENTITY EMAIL ADDRESS]**	Texas Kaixingda Technology Development, LLC dba Sunny & Saima Assisted Living Homes 1109 Holly Street La Marque, Texas 77568 Attention: **[BA CONTACT NAME AND TITLE]** Email: **[BA EMAIL ADDRESS]**

Either party may change its address for notices by providing written notice to the other party in accordance with this Section, effective upon receipt.

11.10 Relationship of the Parties

Nothing in this Agreement shall be construed to create a partnership, joint venture, employment, or agency relationship between the parties. Business Associate is and shall remain an independent contractor. Business Associate shall have no authority to bind Covered Entity to any contract or obligation. Neither party is authorized to act as agent for the other party for any purpose without the other party's prior written consent.

11.11 Force Majeure

Notwithstanding any other provision of this Agreement, a party shall not be deemed to be in breach of this Agreement to the extent that its performance is delayed or prevented by reason of any cause beyond its reasonable control (a **"Force Majeure Event"**), including acts of God, natural disasters, pandemic, war, terrorism, labor strikes, governmental orders, or failures of telecommunications or internet infrastructure, provided that: (a) the affected party provides written notice to the other party as soon as practicable after the occurrence of the Force Majeure Event; (b) the affected party uses its reasonable best efforts to perform its obligations notwithstanding such event; and (c) a Force Majeure Event shall not excuse Business Associate's obligation to maintain the security of PHI or to notify Covered Entity of a Breach or Security Incident, except to the extent performance is rendered physically impossible.

Section 12. Signatures

IN WITNESS WHEREOF, the parties hereto have executed this Business Associate Agreement as of the Effective Date first written above, by their respective authorized representatives.

> ⓘ **Attorney Note**
>
> Confirm that each signatory has actual authority to bind the respective entity before execution. If the Services Agreement requires countersignature or board authorization, verify compliance with the applicable organizational documents of each party prior to execution.

Covered Entity: [COVERED ENTITY LEGAL NAME] [COVERED ENTITY ADDRESS, CITY, STATE, ZIP] Signature: Printed Name: Title: Date:	**Business Associate: Texas Kaixingda Technology Development, LLC dba Sunny & Saima Assisted Living Homes** 1109 Holly Street, La Marque, Texas 77568 Signature: Printed Name: Title: Date:

Exhibit A: Summary of Key Obligations

This table is provided for reference only. In the event of any conflict between this Exhibit and the body of the Agreement, the body of the Agreement shall control.

Obligation	Requirement	Governing Provision
Permitted Uses of PHI	Care delivery platform, compliance reporting, authorized health care operations, as required by law	§ 3.1; 45 C.F.R. § 164.504(e)
Encryption in Transit	TLS 1.2 or higher; no legacy SSL/TLS protocols	§ 3.3(a); § 7.4(a)
Encryption at Rest	AES-256 on all servers, devices, and media	§ 3.3(b); § 7.4(b)
Access Control	Role-Based Access Control (RBAC); least privilege	§ 3.3(c); § 7.4(c)
Multi-Factor Authentication	Required for all personnel accessing ePHI; no exceptions without written justification	§ 3.3(d); § 7.4(d)
Audit Logging	All access and modifications to ePHI; 6-year retention	§ 3.3(e); § 7.4(e)
Breach Notification to CE	Within 5 business days of discovery	§ 3.4.1; § 6.2; 45 C.F.R. § 164.410
Security Incident Reporting	Within 72 hours (non-Breach incidents)	§ 3.4.2
Subcontractor BAAs	Required prior to PHI disclosure; BA fully liable for subcontractors	§ 3.5; § 8.1; 45 C.F.R. § 164.308(b)(2)
Annual Risk Assessment	Minimum annually; results available to CE on request	§ 3.3(f); § 7.6; 45 C.F.R. § 164.308(a)(1)
Individual Rights Support	Access, amendment, accounting — within 10 business days of CE request	§ 3.6; 45 C.F.R. §§ 164.524, 164.526, 164.528

Obligation	Requirement	Governing Provision
Return/Destruction of PHI	Within 45 days of termination; written certification required	§ 5.4.1
Security Attestation	Within 30 days of CE's written request; once per calendar year	§ 7.7
Indemnification	Full indemnification for BA breaches and HIPAA violations	§ 10.1
Governing Law	State of Texas; federal HIPAA law supersedes	§ 11.4
