# HIPAA BUSINESS ASSOCIATE AGREEMENT

## TO THE MASTER SERVICE AGREEMENT

**NOTICE:** This Business Associate Agreement has been prepared by and on behalf of Service Provider. It is intended to satisfy the requirements of 45 C.F.R. § 164.504(e) while preserving the rights and limiting the liabilities of Service Provider. Covered Entity is advised to seek independent legal counsel prior to execution.

This HIPAA Business Associate Agreement ("BAA" or "Agreement") is entered into as of the date of last signature set forth in the signature block below (the "Effective Date") by and between the Covered Entity identified and executing this Agreement in the signature block below ("Covered Entity"), and the Service Provider identified and executing this Agreement in the signature block below ("Service Provider" or "Business Associate"). This Agreement is a separate, standalone document that supplements, but does not replace or modify, the Master Services Agreement between the parties, together with any Statements of Work, Addendums, or other documents incorporated into the MSA that define the scope of services provided to Covered Entity (collectively, the "Service Agreements"). Execution of this Agreement is required only where Covered Entity's operations involve Protected Health Information as described herein. The MSA shall remain in full force and effect independently of this Agreement and does not require the execution of this Agreement to be valid and enforceable.

### RECITALS

WHEREAS, Service Provider provides certain managed information technology services to Covered Entity pursuant to the Service Agreements, which may involve access to Protected Health Information;

WHEREAS, the MSA is a standalone agreement governing the full scope of services between the parties and is not conditioned upon, nor does it incorporate, the terms of this Agreement;

WHEREAS, Covered Entity has disclosed that its operations may involve Protected Health Information, thereby requiring the execution of this supplemental Agreement;

WHEREAS, Service Provider may qualify as a "business associate" as defined under HIPAA solely to the extent that its provision of services under the Service Agreements results in access to PHI; and

WHEREAS, the parties wish to set forth, in this separate and supplemental document, the limited terms and conditions governing Service Provider's HIPAA-related obligations, without modifying any other term of the Service Agreements.

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

### *1. Definitions*

**1.1 "HIPAA Rules"** means, collectively, the Privacy Rule, Security Rule, Breach Notification Rule, and Enforcement Rule at 45 C.F.R. Parts 160 and 164, as amended from time to time.

**1.2 "Protected Health Information" or "PHI"** has the meaning set forth at 45 C.F.R. § 160.103, and for purposes of this Agreement is limited to individually identifiable health information that Service Provider accesses in the course of providing services described in the Service Agreements. PHI does not include information that Service Provider creates, generates, or manages independently of the services provided under the Service Agreements.

**1.3 "Electronic Protected Health Information" or "ePHI"** means PHI that is transmitted or maintained in electronic media, as defined at 45 C.F.R. § 160.103.

**1.4 "Breach"** has the meaning set forth at 45 C.F.R. § 164.402. For purposes of this Agreement, a Breach shall not include any acquisition, access, use, or disclosure of PHI that results from Covered Entity's own acts or omissions, including but not limited to Covered Entity's failure to implement reasonable security practices, failure to restrict access to PHI, or failure to notify Service Provider of the existence or location of PHI.

**1.5 "Client-Caused Incident"** means any security incident, data breach, unauthorized access, or other adverse event involving PHI that arises from or is attributable to: (a) Covered Entity's own negligence, acts, or omissions; (b) Covered Entity's failure to disclose the existence or location of PHI to Service Provider; (c) Covered Entity's failure to implement security measures recommended by Service Provider; (d) actions of Covered Entity's employees, contractors, or agents; or (e) Covered Entity's use of third-party systems, software, or services not managed by Service Provider.

### *2. Scope and Nature of Service Provider's Role*

**2.1 Nature of Service Provider's Access to PHI.** Service Provider's status as a Business Associate arises from its provision of managed information technology services under the Service Agreements, which may result in access to PHI that is incidental, persistent, or ongoing depending on the nature of the services provided. Such services may include, without limitation, the management of backups, cloud environments, hosted infrastructure, disaster recovery systems, endpoint devices, and network environments in which PHI may reside. Regardless of the nature or frequency of such access, Service Provider does not actively create, compile, analyze, or manage PHI as a primary function of its services, and its role remains that of a technology services provider. Covered Entity acknowledges that Service Provider's services are information technology services and not healthcare services.

**2.2 Minimum Necessary Standard.** Covered Entity is solely responsible for ensuring that PHI is segregated, access-controlled, and protected within its own environment. Service Provider shall make reasonable efforts to limit its access to PHI to the minimum necessary to perform the services under the Service Agreements, but shall have no obligation to independently identify, locate, or inventory PHI within Covered Entity's systems.

**2.3 No Healthcare Compliance Advisory.** Nothing in this Agreement shall be construed as Service Provider providing legal, compliance, or regulatory advice regarding HIPAA or any applicable healthcare law. Covered Entity is solely responsible for its own HIPAA compliance obligations and is advised to seek qualified legal counsel. Service Provider makes no representation or warranty that its services, systems, or practices constitute or will result in HIPAA compliance for Covered Entity or for Service Provider. Execution of this Agreement does not certify, guarantee, or imply that Service Provider has achieved or maintains any level of HIPAA certification or compliance.

### *3. Obligations of Service Provider*

**3.1 Permitted Use and Disclosure.** Service Provider shall not use or disclose PHI other than as necessary to perform the services described in the Service Agreements, as permitted or required by this Agreement, or as required by applicable law.

**3.2 Safeguards.** Service Provider shall implement reasonable and appropriate administrative, physical, and technical safeguards within the scope of its Managed Services activities as defined in the Service Agreements, to protect PHI encountered in the course of providing such services from unauthorized use or disclosure. Service Provider's safeguard obligations are strictly limited to those systems and environments under its direct management pursuant to the Service Agreements. Service Provider shall have no responsibility for HIPAA compliance, PHI security, or the implementation of safeguards beyond the scope of its Managed Services activities, unless such responsibility is

specifically and expressly defined in a signed Service Agreement. Nothing in this Section shall be construed to make Service Provider responsible for Covered Entity's overall HIPAA compliance program, policies, workforce training, or any systems or environments not managed by Service Provider under the Service Agreements.

**3.3 Subcontractors and Third-Party Services.** For purposes of this Agreement, "subcontractor" means any third party engaged directly by Service Provider whose work under the Service Agreements results in that party creating, receiving, maintaining, or transmitting PHI on Service Provider's behalf. Service Provider shall use commercially reasonable efforts to verify that any such subcontractor maintains HIPAA-compliant practices, which may include reviewing publicly available Business Associate Agreement terms, privacy policies, security certifications, or attestations provided by such third party. Service Provider does not warrant or guarantee the HIPAA compliance of any third-party subcontractor, platform, or service provider, and shall have no liability for the acts or omissions of any such party except to the extent directly caused by Service Provider's own gross negligence or willful misconduct in selecting or instructing such party. This Section does not extend to any vendors, platforms, or service providers engaged directly by Covered Entity, for whom Covered Entity remains solely responsible.

**3.4 Breach Notification.** Upon discovery of a confirmed or reasonably suspected Breach of Unsecured PHI arising directly from Service Provider's own acts or omissions, Service Provider shall: (a) provide Covered Entity with written preliminary notice within ten (10) calendar days of discovery, identifying the nature of the potential Breach, the categories of PHI potentially involved, and any immediate containment steps taken; and (b) provide Covered Entity with a full written Breach notification within sixty (60) calendar days of discovery, including to the extent then available the information required by 45 C.F.R. § 164.410(c). The preliminary notice satisfies Service Provider's obligation to notify without unreasonable delay under the HIPAA Breach Notification Rule, and the sixty (60) day period shall govern the timing of the full report. Service Provider shall have no obligation to notify Covered Entity of Client-Caused Incidents, though Service Provider may at its discretion provide courtesy notification. Service Provider's notification obligations under this Section are limited to notifying Covered Entity of a Breach. All obligations to notify affected individuals, the Secretary of HHS, the media, or any other party under 45 C.F.R. §§ 164.404, 164.406, and 164.408 are solely the responsibility of Covered Entity, and Service Provider shall have no obligation to perform, fund, or manage such notifications. In addition to the foregoing, the parties' respective rights, liabilities, limitations, and obligations with respect to any Breach, security incident, or cyberattack—including but not limited to liability caps, exclusions, incident response services, and associated costs—shall be governed by the Data Breach Liability provisions of the MSA, which are incorporated herein by reference. To the extent of any conflict between this Section and the MSA's Data Breach Liability provisions, the MSA shall control.

**3.4a Security Incidents.** Service Provider shall track attempted and successful Security Incidents, as defined at 45 C.F.R. § 164.304, of which it becomes aware in the course of providing services under the Service Agreements. Not every Security Incident constitutes a Breach requiring formal notification under Section 3.4. Service Provider shall report to Covered Entity only those Security Incidents that, upon reasonable investigation, meet the definition of a Breach of Unsecured PHI under the HIPAA Rules. Routine Security Incidents that do not rise to the level of a Breach—including but not limited to unsuccessful access attempts, port scans, malware blocked by security controls, and similar low-level events—shall be tracked internally by Service Provider but shall not trigger the notification obligations set forth in Section 3.4. Covered Entity acknowledges that demanding formal Breach notification for Security Incidents that do not meet the regulatory threshold is not required under HIPAA and shall not constitute a basis for claiming Service Provider has breached this Agreement.

**3.5 Access and Amendment.** To the extent Service Provider maintains PHI in a Designated Record Set, Service Provider shall make such PHI available to Covered Entity for access or amendment as

required by 45 C.F.R. §§ 164.524 and 164.526. Service Provider shall have no obligation to maintain PHI in a Designated Record Set unless expressly required to do so under the Service Agreements.

**3.6 Accounting of Disclosures.** To the extent required by applicable law and permitted by 45 C.F.R. § 164.528, Service Provider shall maintain records of accountable disclosures of PHI belonging solely to Covered Entity under this Agreement, and shall provide such records to Covered Entity within a reasonable time following a written request. This obligation is strictly limited to: (a) disclosures made directly by Service Provider in the performance of services under the Service Agreements; (b) PHI belonging to Covered Entity as the named party to this Agreement; and (c) disclosures that are not otherwise exempt from the accounting requirement under the HIPAA Rules or applicable law. Service Provider shall have no obligation to account for disclosures made by Covered Entity, its employees, contractors, agents, or any of Covered Entity's own third-party vendors, nor for any disclosures that are exempt under 45 C.F.R. § 164.528(a)(1).

**3.7 Government Access.** Service Provider shall make its internal practices, books, and records relating to its use and disclosure of PHI available to the Secretary of HHS for purposes of determining Covered Entity's compliance with the HIPAA Rules, as required by law. To the extent permitted by law, Service Provider shall promptly notify Covered Entity of any such governmental request.

### *4. Obligations of Covered Entity*

**4.1 Disclosure of PHI Locations.** Covered Entity shall promptly disclose to Service Provider, in writing, the existence and location of all PHI within any systems or environments managed by Service Provider. Covered Entity's failure to disclose the existence or location of PHI shall relieve Service Provider of any obligation under this Agreement with respect to such undisclosed PHI, and Covered Entity shall indemnify Service Provider for any resulting liability.

**4.2 Lawful Instructions.** Covered Entity shall not instruct Service Provider to use or disclose PHI in any manner that would violate the HIPAA Rules if done by Covered Entity. Covered Entity shall be solely responsible for ensuring that its instructions to Service Provider comply with applicable law.

**4.3 Security Practices.** Covered Entity shall implement and maintain reasonable security practices within its own environment, including but not limited to access controls, user authentication, and endpoint security. Covered Entity's failure to implement such practices, where such failure contributes to a security incident or Breach, shall constitute a Client-Caused Incident and shall relieve Service Provider of liability to the extent of such contribution.

**4.4 Employee and Contractor Conduct.** Covered Entity is solely responsible for the conduct of its employees, contractors, and agents with respect to PHI. Any Breach or security incident caused by Covered Entity's employees, contractors, or agents shall constitute a Client-Caused Incident.

**4.5 HIPAA Compliance.** Covered Entity is solely responsible for its own compliance with HIPAA and all applicable federal and state healthcare privacy laws. Service Provider's obligations under this Agreement do not constitute, and shall not be construed as, a guarantee of Covered Entity's HIPAA compliance.

### *5. Limitation of Liability*

**5.1 Limitation of Liability. SERVICE PROVIDER'S TOTAL CUMULATIVE LIABILITY TO COVERED ENTITY UNDER THIS AGREEMENT SHALL BE SUBJECT TO AND GOVERNED BY THE LIMITATION OF LIABILITY PROVISIONS SET FORTH IN THE MSA, WHICH ARE INCORPORATED HEREIN BY REFERENCE.**

**5.2 Exclusion of Consequential Damages. IN NO EVENT SHALL SERVICE PROVIDER BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE, OR EXEMPLARY DAMAGES, INCLUDING BUT NOT LIMITED TO LOSS OF REVENUE, LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF GOODWILL, REGULATORY FINES OR PENALTIES, COSTS OF NOTIFICATION, CREDIT MONITORING, OR LEGAL DEFENSE, ARISING OUT OF OR RELATED TO THIS AGREEMENT, EVEN IF SERVICE PROVIDER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.**

**5.3 Client-Caused Incidents. SERVICE PROVIDER SHALL HAVE NO LIABILITY WHATSOEVER FOR ANY CLIENT-CAUSED INCIDENT AS DEFINED IN SECTION 1.5, INCLUDING BUT NOT LIMITED TO ANY BREACH, SECURITY INCIDENT, OR REGULATORY VIOLATION ARISING FROM COVERED ENTITY'S OWN ACTS OR OMISSIONS, ITS FAILURE TO DISCLOSE PHI LOCATIONS, ITS FAILURE TO IMPLEMENT RECOMMENDED SECURITY MEASURES, OR THE CONDUCT OF ITS EMPLOYEES, CONTRACTORS, OR AGENTS.**

**5.4 Regulatory Fines and Penalties. SERVICE PROVIDER SHALL NOT BE LIABLE FOR ANY REGULATORY FINES, CIVIL MONETARY PENALTIES, OR ENFORCEMENT ACTIONS IMPOSED BY THE DEPARTMENT OF HEALTH AND HUMAN SERVICES, THE OFFICE FOR CIVIL RIGHTS, OR ANY OTHER GOVERNMENTAL AUTHORITY, ARISING FROM COVERED ENTITY'S OWN FAILURE TO COMPLY WITH HIPAA OR ANY OTHER APPLICABLE LAW.**

**5.5 Indemnification by Covered Entity.** Covered Entity shall indemnify, defend, and hold harmless Service Provider and its directors, officers, employees, subcontractors, and agents from and against any and all claims, damages, fines, penalties, costs, and expenses (including reasonable attorneys' fees) arising out of or relating to: (a) any Client-Caused Incident; (b) Covered Entity's failure to disclose the existence or location of PHI; (c) Covered Entity's breach of this Agreement or the HIPAA Rules; (d) Covered Entity's failure to implement security measures recommended by Service Provider; or (e) the conduct of Covered Entity's employees, contractors, or agents with respect to PHI.

**5.6 Indemnification by Service Provider.** Service Provider shall indemnify, defend, and hold harmless Covered Entity and its directors, officers, employees, and agents from and against any and all claims, damages, fines, penalties, costs, and expenses (including reasonable attorneys' fees) arising directly and proximately from Service Provider's gross negligence or willful misconduct in the use or disclosure of PHI under this Agreement. Service Provider's indemnification obligation under this Section is subject to and shall not exceed the limitation of liability set forth in Section 5.1 and the MSA. Service Provider shall have no indemnification obligation for any claim arising from or contributed to by Covered Entity's own acts, omissions, or Client-Caused Incidents.

### *6. Term and Termination*

**6.1 Term.** This Agreement shall become effective as of the Effective Date and shall remain in effect until terminated in accordance with this Section 6, or until the termination or expiration of the MSA, whichever occurs first.

**6.2 Termination for Cause by Service Provider.** Service Provider may terminate this Agreement and suspend services immediately upon written notice to Covered Entity if: (a) Covered Entity materially breaches this Agreement and fails to cure such breach within sixty (60) days after receipt of written notice; (b) Covered Entity instructs Service Provider to use or disclose PHI in a manner that would violate applicable law; or (c) Service Provider reasonably determines that continued performance would expose Service Provider to material legal or regulatory liability.

**6.3 Termination for Cause by Covered Entity.** Covered Entity may terminate this Agreement upon written notice to Service Provider if Service Provider materially breaches this Agreement and fails to cure such breach within sixty (60) days after receipt of written notice specifying the nature of the

breach in reasonable detail. Covered Entity's right to terminate shall not affect Service Provider's right to payment for services rendered prior to termination.

**6.4 Obligations Upon Termination.** Upon termination or expiration of this Agreement, Service Provider shall, with respect to PHI in its possession: (a) return to Covered Entity or, upon written agreement of the parties, securely destroy all PHI that Service Provider can practically return or destroy; (b) retain only that PHI necessary for Service Provider's proper management and administration or to carry out its legal responsibilities; and (c) continue to apply reasonable safeguards to any retained PHI for so long as it is retained. Service Provider's costs associated with returning or destroying PHI shall be billed to Covered Entity at Service Provider's then-current standard rates.

**6.5 Infeasibility.** If return or destruction of PHI is not feasible, Service Provider shall notify Covered Entity in writing and shall extend the protections of this Agreement to such PHI for as long as it is retained, limiting further use or disclosure to the purposes that make return or destruction infeasible.

### *7. General Provisions*

**7.1 Amendment.** The parties agree to amend this Agreement as necessary to comply with changes in HIPAA or other applicable law. Any amendment shall be in writing and signed by both parties. Service Provider reserves the right to propose amendments at any time and Covered Entity agrees to negotiate such amendments in good faith.

**7.2 Relationship to Master Services Agreement.** This Agreement is a standalone, supplemental document that operates alongside the Service Agreements and is required only when Covered Entity's operations involve Protected Health Information. The Service Agreements shall remain in full force and effect independently of this Agreement, and neither the existence nor the execution of this Agreement shall be construed to modify, limit, or expand any term of the Service Agreements. This Agreement governs solely the parties' rights and obligations with respect to PHI and HIPAA compliance. In the event of a conflict between this Agreement and the Service Agreements on matters relating to PHI or HIPAA obligations, this Agreement shall control. In all other respects, including without limitation all provisions governing fees, payment, service levels, limitation of liability, and general indemnification, the Service Agreements shall control exclusively. The termination of the MSA shall automatically terminate this Agreement. The termination of this Agreement shall not affect the validity or enforceability of the Service Agreements.

**7.3 Governing Law.** This Agreement shall be governed by and construed in accordance with the same governing law, jurisdiction, and venue provisions set forth in the MSA, which are incorporated herein by reference. In the event the MSA does not contain a governing law provision, this Agreement shall be governed by the laws of the state in which Service Provider maintains its principal place of business, without regard to conflict-of-law principles, except to the extent preempted by federal law including HIPAA.

**7.4 Interpretation.** Any ambiguity in this Agreement shall be resolved in a manner that is consistent with the HIPAA Rules and that preserves the limitations on Service Provider's liability set forth herein. This Agreement shall not be construed against Service Provider as the drafting party.

**7.5 Survival.** The provisions of Sections 1, 5, 6.4, 6.5, and 7 shall survive the termination or expiration of this Agreement.

**7.6 Severability.** If any provision of this Agreement is found to be invalid or unenforceable, the remaining provisions shall continue in full force and effect.

**7.7 Counterparts.** This Agreement may be executed in counterparts, each of which shall be deemed an original. Electronic and digital signatures shall be deemed valid and binding.

**7.8 No Waiver.** No failure or delay by Service Provider in exercising any right under this Agreement shall constitute a waiver of that right.

**7.9 No Third-Party Beneficiaries; Affiliated Entities.** This Agreement is entered into solely between Service Provider and the named Covered Entity executing this Agreement in the signature block below. No affiliate, subsidiary, parent company, related entity, successor, or assign of Covered Entity is a party to, or a third-party beneficiary of, this Agreement, and no such entity shall have any rights or claims against Service Provider hereunder. This Agreement does not extend BAA coverage to any entity other than the named Covered Entity. Any affiliate, subsidiary, or related entity of Covered Entity that requires Business Associate services or BAA coverage must execute a separate, standalone Business Associate Agreement directly with Service Provider prior to receiving any services that may involve PHI. Covered Entity is solely responsible for ensuring that none of its affiliates, subsidiaries, or related entities access PHI under this Agreement or receive services implicating PHI without a separately executed BAA. Any claim brought against Service Provider by or on behalf of an affiliate, subsidiary, or related entity of Covered Entity that does not have its own executed BAA with Service Provider shall be subject to dismissal, and Covered Entity shall indemnify Service Provider for any costs, including attorneys' fees, incurred in defending such a claim.

**7.10 Data Ownership.** All PHI accessed, received, maintained, or transmitted by Service Provider under this Agreement remains the sole and exclusive property of Covered Entity. Service Provider acquires no right, title, interest, or license in or to any PHI by virtue of this Agreement or the services performed hereunder. Service Provider shall use PHI solely as necessary to perform the services described in the Service Agreements and for no other purpose. Upon termination of this Agreement, all rights to PHI revert exclusively to Covered Entity subject to the retention obligations set forth in Section 6.4.

**7.11 Dispute Resolution.** Any dispute arising out of or relating to this Agreement, including any dispute regarding an alleged Breach, Client-Caused Incident, or the parties' respective notification obligations, shall be resolved in accordance with the dispute resolution provisions set forth in the MSA, which are incorporated herein by reference. Neither party shall initiate formal legal proceedings with respect to any dispute under this Agreement without first following the dispute resolution process set forth in the MSA.

**7.12 Force Majeure.** Service Provider shall not be in breach of this Agreement, and shall have no liability to Covered Entity, for any failure or delay in performing its obligations under this Agreement to the extent such failure or delay is caused by circumstances beyond Service Provider's reasonable control, including but not limited to acts of God, natural disasters, pandemic, government action, cyberattacks on third-party infrastructure providers, internet or telecommunications failures, power outages, or other events that could not have been prevented by the exercise of reasonable diligence. In such circumstances, Service Provider shall: (a) notify Covered Entity as soon as reasonably practicable; (b) use commercially reasonable efforts to resume performance; and (c) implement reasonable interim measures to protect PHI during the period of disruption. Force majeure shall not excuse Service Provider from obligations that arose prior to the force majeure event, nor shall it excuse Client-Caused Incidents.

## SIGNATURES

IN WITNESS WHEREOF, the parties identified below have executed this Business Associate Agreement as of the date of last signature below, which shall constitute the Effective Date of this Agreement.

**SERVICE PROVIDER**

| | |
|---|---|
| Legal Entity Name: | Xirtix Consulting, LLC |
| Entity Type & State of Formation: | Texas |
| | |
| *Signature* | *Date* |
| | |
| *Name* | *Title* |

**COVERED ENTITY (CLIENT)**

| | |
|---|---|
| Legal Entity Name: | |
| Entity Type & State of Formation: | |
| | |
| *Signature* | *Date* |
| | |
| *Name* | *Title* |