**Business Associate Agreement**

This Business Associate Agreement (“**Agreement**”) is entered into on Enter Effective Date (the “**Effective Date**”), by and between Arthur J. Gallagher & Co. as Plan Sponsor of the Arthur J. Gallagher & Co. Employee’s Self-Funded Medical/Dental Plan and Insured Benefits (**“Gallagher**”) and Insert Vendor Name (“**Business Associate**”).

**RECITALS**

**WHEREAS,** Business Associate provides, or intends to provide certain products or services to Gallagher described in an underlying service agreement (“**Service Agreement**”) which services or products may involve the exchange of Protected Health Information (“**PHI**”) and by reason of such activities, Business Associate is a “business associate” of a “covered entity”, as such terms are defined in 45 C.F.R. § 160.103;

**WHEREAS**, Gallagher and Business Associate mutually desire to outline their individual responsibilities with respect to the use, disclosure and security of any PHI that Business Associate accesses in connection with the Service Agreement and to ensure Gallagher and Business Associate comply with the applicable requirements of the Health Insurance Portability and Accountability Act of 1996, as codified at 42 U.S.C. § 1320d (“**HIPAA**”), the Health Information Technology for Economic and Clinical Health Act of 2009, as codified at 42 U.S.C. § 17901 *et seq.* (“**HITECH Act**”), and any current and future regulations promulgated under HIPAA or the HITECH Act, including without limitation, the Confidentiality of Substance Use Disorder Patient Records, 42 C.F.R. Part 2 (“**Part 2**”) (HIPAA, HITECH Act, and any current and future regulations promulgated under either are collectively referred to as the “**Regulations**”); and

**WHEREAS**, Gallagher and Business Associate understand and agree that the Regulations require them to enter into this Agreement, which shall govern the use, disclosure and security of PHI.

**NOW, THEREFORE,** the parties hereto agree as follows:

# **Definitions.** When used in this Agreement and capitalized, the following terms have the following meanings:

## “**Breach**” shall have the same meaning as the term “breach” in 45 C.F.R. § 164.402.

## “**Electronic Protected Health Information**” or “**ePHI**” shall mean Protected Health Information transmitted by electronic media or maintained in electronic media.

## “**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).

## “**Privacy Rule**” shall mean the Standards for Privacy of Individual Identifiable Health Information as set forth at 45 C.F.R. Parts 160 and 164 Subparts A and E.

## “**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 the information created or received by Business Associate from or on behalf of Gallagher.

## “**Required by Law**” shall have the same meaning as the term “required by law” in 45 C.F.R. § 164.103.

## “**Secretary**” shall mean the Secretary of the Department of Health and Human Services or his or her designee.

## “**Security Incident**”shall have the same meaning as the term “security incident” in 45 C.F.R. § 164.304.

## “**Security Rule**” shall mean the Standards for Security of PHI, including ePHI, as set forth at 45 C.F.R. Parts 160 and 164 Subparts A and C.

## “**Unsecured PHI**” shall have the same meaning as the term “unsecured protected health information” in 45 C.F.R. § 164.402.

Capitalized terms used but not defined in this Agreement shall have the same meaning as those terms in the Regulations.

# **Obligations and Activities of Business Associate Regarding PHI.**

## Business Associate shall comply with its obligations under the Regulations with respect to its use, disclosure and security of PHI.

## Business Associate shall use appropriate safeguards to comply with the Security Rule, to prevent the use or disclosure of the PHI other than as provided for by this Agreement.

## Business Associate shall provide reasonable and appropriate training to its employees to ensure compliance with this Agreement and the Regulations.

## Business Associate shall ensure that any agents and sub-contractors that create, receive, maintain or transmit PHI on behalf of Business Associate agree to comply with the same restrictions, conditions and requirements that apply to Business Associate with respect to such information. Business Associate shall enter into written agreements with any such agents and subcontractors, and the terms of such agreements shall incorporate the applicable requirements of, and otherwise comply with, the Regulations.

## Upon request of Gallagher and in the time and manner designated by Gallagher, Business Associate shall:

### provide Gallagher with access to PHI in a Designated Record Set in order for Gallagher to meet the requirements under 45 C.F.R. § 164.524;

### make any amendments to PHI in a Designated Record Set that Gallagher directs or agrees to pursuant to 45 C.F.R. § 164.526; and

### provide Gallagher with documentation of any disclosures by Business Associate in order for Gallagher to comply with its obligation to provide an accounting of disclosures to an Individual under 45 C.F.R. § 164.528.

## Business Associate shall give notice to Gallagher, as soon as reasonably practical but no later than five (5) business days after receipt, of any request under 45 C.F.R. §§ 164.524, 164.526 or 164.528 that it receives directly from an Individual and shall provide reasonable cooperation and assistance to Gallagher in order for Gallagher to comply with its requirements under the Regulations.

## To the extent Business Associate performs any of Gallagher’s obligations under the Privacy Rule, Business Associate shall comply with the requirements of the Privacy Rule that apply to Gallagher in the performance of such obligations.

## Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI available to Gallagher for the purpose of determining Business Associate’s compliance with this Agreement and the Regulations, and to the Secretary for purposes of the Secretary determining Business Associate’s or Gallagher’s compliance with the Regulations. Business Associate shall make such information available within thirty (30) days of the request, or such earlier time as required by the Secretary. Business Associate shall notify Gallagher as soon as reasonably practical but no later than two (2) business days after its receipt or notice of any such request by the Secretary.

# **Permitted Uses and Disclosures of PHI by Business Associate.**

## Business Associate may use or disclose PHI only as necessary to provide the products or services under the Service Agreement, as permitted under this Agreement, or as Required by Law.

## Business Associate must not use or disclose PHI in a manner that is prohibited under the Privacy Rule, 45 C.F.R. § 164.502(a)(5) or Part 2, or would otherwise violate the Privacy Rule or Part 2 if done by Gallagher, except for the specific uses and disclosures permitted below.

## Business Associate may use PHI for the proper management and administration of its business and to carry out its legal responsibilities.

## Business Associate may disclose PHI for the proper management and administration of its business and to carry out its legal responsibilities if:

### Such disclosure is Required by Law, or

### Business Associate obtains reasonable assurances from the person to whom the information is disclosed that such information will remain confidential and used or further disclosed only as Required by Law or for the purposes for which it was disclosed to the person, and the person agrees to notify Business Associate of any instances of which it is aware that the confidentiality of the information has been Breached.

## Business Associate must not sell, sub-license or receive any remuneration from a third party for PHI and must not use or disclose PHI for any marketing activities, without Gallagher’s prior written consent. Any permitted use must be in accordance with the Privacy Rule.

## Business Associate shall limit its uses and disclosures of, and requests for, PHI, to the minimum amount of PHI necessary to accomplish the intended purpose of such use, disclosure or request subject to the exceptions set forth in the Privacy Rule.

## To the extent necessary to provide the services or products under the Service Agreement, Business Associate may use PHI to provide Data Aggregation services related to the health care operations of Gallagher as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B). If Business Associate is de-identifying PHI as part of the Data Aggregation services for Gallagher, Business Associate must comply with the de-identification standards of 45 C.F.R. § 164.514.

## Business Associate must not use any PHI, even if de-identified, for any improvements or enhancements to Business Associate’s services, offerings, product development or any other business interest without prior written approval from Gallagher.

## Business Associate shall comply with any requests for restrictions on certain uses and disclosures of PHI to which Gallagher has agreed in accordance with 45 C.F.R. § 164.522 and of which Business Associate has been notified by Gallagher.

# **Security of Protected Health Information.**

## Business Associate has implemented policies and procedures to ensure that its creation, receipt, maintenance or transmission of PHI complies with the administrative, physical and technical safeguards of the Security Rule and protects the confidentiality, availability and integrity of PHI, including:

### Business Associate has implemented all required specifications as set out in the Security Rule;

### Where the Security Rule has categorized an implementation specification as “addressable”, Business Associate has analyzed whether such specification constitutes a reasonable and appropriate safeguard that is likely to contribute to protecting PHI. Based on that analysis, Business Associate must either (i) implement the specification as set forth in the Security Rule; or (ii) document why Business Associate has determined that implementation of the specification is not reasonable and appropriate and implement an equivalent alternative measure that will adequately protect PHI and provide such information to Gallagher upon request.

## Business Associate shall ensure that its agents or subcontractors agree to implement the administrative, physical and technical safeguards as set out in the Security Rule to protect the confidentiality, availability and integrity of PHI, consistent with Business Associate’s obligations as set forth in section (a) above.

## Business Associate shall secure in transit all PHI by a technology standard that renders PHI unusable, unreadable or indecipherable to unauthorized individuals consistent with any guidance issued by the Secretary, including the use of standards developed under Section 3002(b)(2)(B)(vi) of the Public Health Service Act, as added by the HITECH Act, and any other guidance which may be issued from time to time.

## Business Associate shall establish procedures to mitigate, to the extent possible, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate or its agents or subcontractors in violation of this Agreement.

## Business Associate agrees to notify Gallagher as soon as practicable, but not later than two (2) business days after Discovery (as defined by 45 C.F.R. § 164.410) of any Security Incident, Breach of Unsecured PHI or any breach of this Agreement and, to the extent available to Business Associate, provide the following information relating to a Breach of Unsecured PHI to Gallagher:

### The date of the Breach;

### The date of the discovery of the Breach;

### A description of the type of Unsecured PHI that was involved;

### The identity of each Individual whose Unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed; and

### Any other information reasonably requested by Gallagher to permit Gallagher to comply with the requirements of 45 C.F.R. Part 164 Subpart D.

## Upon request by Gallagher, Business Associate will provide notifications to Individuals whose Unsecured PHI has been disclosed, as well as to the Secretary and the media, to the extent required, provided that Business Associate shall not provide any such notification on behalf of Gallagher without the prior written consent of Gallagher.

## Business Associate shall be responsible for all costs, fees or expenses incurred in connection with a Security Incident or Breach, including but not limited to, notifications and credit monitoring costs, reasonable attorneys’ fees, forensic investigation fees and mitigation activities that Gallagher determines are necessary or appropriate, except to the extent that Business Associate or its agents or subcontractors were not responsible for or did not contribute to or cause the Security Incident or Breach.

# **Term and Termination.**

## **Term**.This Agreement shall be effective as of the Effective Date and shall remain in effect until this Agreement is terminated and all PHI is returned or destroyed.

## **Termination for Cause by Gallagher**. Upon Gallagher’s knowledge of a material breach of this Agreement by Business Associate, Gallagher shall have the right to immediately terminate this Agreement and the underlying Service Agreement between Gallagher and Business Associate.

## **Effect of Termination**. Upon termination of this Agreement, Business Associate shall, within thirty (30) days and as directed by Gallagher:

### Return or destroy all PHI received from Gallagher, or created or received by Business Associate on behalf of Gallagher, or, alternatively, transfer all PHI to a third party; and

### Instruct its agents and sub-contractors to return, destroy or transfer all PHI received from Business Associate; and

### Confirm in writing that all PHI in its possession or the possession of its agents or subcontractors has been returned, destroyed or transferred.

## **Survival.** The obligations of Business Associate under this Agreement shall survive the termination of this Agreement until all PHI is returned, destroyed or transferred.

# **Amendment.**

The parties may agree to amend this Agreement from time to time as is necessary for compliance with the requirements of the Regulations, other applicable laws and any other respect that they deem appropriate. This Agreement shall only be amended by written instrument executed by the parties.

# **Indemnification.**

Business Associate shall indemnify and hold harmless Gallagher from and against any and all costs, expenses, claims, demands, causes of action, damages, attorneys’ fees and judgments (including, without limitation, reasonable legal expenses, forensic investigation fees, notification costs and credit and identity monitoring services for a period of two (2) years for affected Individuals and the costs to enforce its indemnity rights under this Addendum or to pursue its rights against any insurance providers) that arise out of or that may be imposed upon, incurred by or brought against Gallagher to the extent directly resulting from a breach of this Agreement, a Security Incident, a Breach or any act or omission related to this Agreement determined to constitute negligence, fraud, misrepresentation or a violation of the Regulations or any other law by Business Associate or its agents or subcontractors. The indemnification obligations provided for in this Section will commence on the Effective Date of this Agreement and will survive its termination.

# **Severability.**

The parties intend this Agreement to be enforced as written. Should any provision of this Agreement be held unenforceable or invalid under the laws of any jurisdiction, then the parties agree that the remaining provisions of the Agreement shall be severed therefrom and unaffected thereby, and that this Agreement, without the unenforceable or invalid provisions, shall remain in full force and effect.

# **Notices.**

## The following are the primary contacts for purposes of any co-operation, communications or notices with respect to this Agreement:

### [Name of Business Associate] contact:

[Name], [Title], [Phone], [E-mail]

### Gallagher contact for Security Incidents or Breaches of Unsecured PHI: [cyber\_security@ajg.com](mailto:cyber_security@ajg.com).

### Gallagher contact for all other communications or notices relating to this Agreement: [GlobalPrivacyOffice@ajg.com](mailto:GlobalPrivacyOffice@ajg.com).

## Each party shall promptly notify the other if any of the above contact information changes.

# **Regulatory References.**

A reference in this Agreement to a section in the Regulations means the referenced section or its successor, and for which compliance is required.

# **Headings and Captions.**

The headings and captions of the various subdivisions of the Agreement are for convenience or reference only and will in no way modify or affect the meaning or construction of any of the terms or provisions hereof.

# **Entire Agreement.**

This Agreement sets forth the entire understanding of the parties with respect to the subject matter herein and supersedes all prior agreements, arrangements, and communications, whether oral or written, pertaining to the subject matter hereof. In the event of any conflict between the terms and conditions of this Agreement and the Service Agreement, the terms and conditions of this Agreement shall prevail.

# **Binding Effect.**

# The provisions of this Agreement shall be binding upon and shall inure to the benefit of both parties and their respective successors and assigns.

# **No Waiver.**

# No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions by either party shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.

# **Governing Law.**

This Agreement will be governed by and construed in accordance with the laws of the State of Illinois.

**IN WITNESS WHEREOF**, the parties have executed this Business Associate Agreement as of the Effective Date.

|  |
| --- |
| **BUSINESS ASSOCIATE:** |
| Insert Business Associate Name  By:  Name:  Title: |
| **COVERED ENTITY:**  Arthur J. Gallagher & Co. as Plan Sponsor of the Arthur J. Gallagher & Co. Employee’s Self-Funded Medical/Dental Plan and Insured Benefits  By:  Name:  Title: |