Business Associate Agreement

This Business Associate Agreement ("**BAA**") is entered into as of t _____ (the "**Effective Date**"), by and between _____ (referred to in this BAA as "**Covered Entity**"), and Johnson & Johnson Vision Care, Inc. (referred to in this BAA as "**Business Associate**").

RECITALS

WHEREAS, Business Associate is providing the **MyACUVUE Subscription Program** and/or the **Acuvue Checkout and Shop programs** for Covered Entity's Health Care Operations and Treatment purposes, as specified in the Agreement ("**Services**"), which Services may involve the use and/or disclosure of Protected Health Information ("**PHI**") (defined below); and

WHEREAS, the parties desire to enter into this BAA in order to comply with the provisions of HIPAA that are applicable to Business Associate, as well as any amendments or additions thereto, including amendments made by the HITECH Act and GINA (defined below);

WHEREAS, nothing herein constitutes an admission that either party is a subject to HIPAA, the HITECH Act or GINA, or is a covered entity or business associate under HIPAA, except as required by law;

NOW, THEREFORE, in consideration of these premises and the mutual promises and undertakings herein contained, the parties agree as follows:

1. Terms. Capitalized terms used but not otherwise defined in this BAA or the Agreement shall have the same meaning as those terms in 45 CFR Parts 160 and 164.

1.1. Breach Notification Rule. The term "**Breach Notification Rule**" shall mean the requirements concerning Notification in the Case of Breach of Unsecured Protected Health Information, as codified at 45 CFR Part 164, Subpart D.

1.2. Data Aggregation. The term "**Data Aggregation**" shall have the meaning assigned to such a term in 45 CFR § 164.501, and includes, but is not limited to, combining PHI created or received to permit data analysis services for Covered Entity as specified in a written agreement and consistent with this BAA.

1.3. Designated Record Set. The term "**Designated Record Set**" shall have the meaning assigned to such term in 45 CFR § 164.501, but shall be limited to any item, collection or grouping of PHI maintained, created, or received by or for Covered Entity.

1.4. Electronic Protected Health Information or EPHI. The term "**Electronic Protected Health Information**" or "**EPHI**" shall have the meaning assigned to such term in 45 CFR § 160.103, limited however, to the information that Business Associate creates, accesses, or receives in connection with this BAA or in connection with the Services conducted by Business Associates with respect to patients of Covered Entity.

1.5. GINA. The term "**GINA**" shall mean the Genetic Information Nondiscrimination Act of 2008 and any implementing regulations or guidance thereunder.

1.6. HIPAA. The term "**HIPAA**" shall mean HIPAA, as defined in the Agreement, and as modified and amended, and its implementing regulations, sometimes referred to as the "Privacy Rule," "Security Rule," and "Breach Notification Rule," and incorporating any amendments thereto made by the HITECH Act, GINA, and other applicable laws or regulations.

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

1.8. **Privacy Rule.** The term "**Privacy Rule**" shall mean the requirements concerning Privacy of Individually Identifiable Health Information as codified at 45 CFR Part 160 and Subparts A and E of 45 CFR Part 164.

1.9. **Protected Health Information or PHI.** The term "**Protected Health Information**" or "**PHI**" shall have the meaning set forth in 45 CFR § 160.103, limited however, to the information that Business Associate creates, accesses, or receives in connection with this BAA or in connection with the Services conducted by Business Associate with respect to patients of Covered Entity. PHI includes EPHI.

1.10. **Secretary.** The term "**Secretary**" shall mean the Secretary of the Department of Health and Human Services.

1.11. **Security Rule.** The term "**Security Rule**" shall mean the Security Standards for the Protection of Electronic Health Information as codified at 45 CFR Part 160 and Subparts A and C of 45 CFR Part 164.

1.12. **Services.** The term "**Services**" shall mean the data analysis, analytics, and related services that Business Associate performs for Covered Entity, as specified in the program's Terms & Conditions. The Services are necessary for Covered Entity's Health Care Operations purposes including, but not limited to, business planning and development; cost management and planning related analyses relating to managing and operating Covered Entity, and business management and general administrative activities of Covered Entity. The Services are also necessary for Covered Entity's Treatment purposes including, but not limited to, coordination and management of health care and related services, including helping to ensure that appropriate devices and products are available as needed for patient procedures.

1.13. **Unsecured Protected Health Information or Unsecured PHI.** The term "**Unsecured Protected Health Information**" or "**Unsecured PHI**" shall have the meaning assigned to such term in 45 CFR § 164.402, limited however, to the information that Business Associate creates, accesses, or receives in connection with this BAA or in connection with reimbursement investigation services conducted by Business Associate with respect to patients of Covered Entity.

2. Business Associate Obligations.

2.1. **Use and Disclosure.** Business Associate shall not use or disclose PHI other than (a) as necessary to perform the Services, (b) as otherwise expressly permitted in this BAA or the Agreement, or (c) as Required by Law and in accordance with Section 2.3 (Use and Disclosures Required By Law) of this BAA. Business Associate shall not use or disclose PHI in any manner that violates HIPAA, the HITECH Act, GINA, or any other applicable federal or state laws and regulations relating to the privacy and security of PHI.

2.2. **Certain Permitted Uses and Disclosures.** In accordance with 45 CFR §§ 164.504(e)(2)(i) and 164.504(e)(4), Business Associate may use or disclose PHI if expressly permitted in this BAA or the Terms & Conditions, or such use or disclosure is necessary (a) for the proper management and administration of Business Associate; (b) to provide Data Aggregation services relating to the Health Care Operations of the Covered Entity; (c) to use PHI, including, but not limited to, aggregated PHI, to create, or to have its Subcontractors create, de-identified data which is no longer subject to this BAA or the Agreement and may be used and disclosed, on a royalty-free basis, as Business Associate deems appropriate; or (d) to carry out the legal responsibilities of Business Associate; provided, however, that any permitted disclosure of PHI to a third party must be either Required By Law or subject to reasonable assurances obtained by Business Associate from the third party that the PHI will be held

confidentially and used or further disclosed only as Required By Law or for the purposes for which it was disclosed to such third party, and that any breaches of confidentiality of the PHI which become known to such third party will be immediately reported to Business Associate.

2.3. **Uses and Disclosures Required By Law.** Business Associate may use and disclose PHI to the extent such use or disclosure is Required By Law provided (a) the use or disclosure complies with and is limited to the relevant requirements of such law, and (b) the use or disclosure complies with the requirements of 45 CFR § 164.512(a) to the same extent such requirements would apply if the use or disclosure were made by Covered Entity.

2.4. **Minimum Necessary.** Business Associate agrees to follow any applicable guidance issued by the Department of Health and Human Services regarding what constitutes "minimum necessary" with respect to the use or disclosure of PHI. Until the time that any such guidance is issued, Business Associate shall limit its use or disclosure of PHI, to the extent practicable, to a limited data set (as defined in section 45 CFR § 164.514(e)(2)) or, to the minimum necessary to accomplish the intended purpose of such use or disclosure.

2.5. **Security of EPHI.** Business Associate agrees to comply with Subpart C of 45 CFR Part 164 including the applicable standards of 45 CFR § § 164.306, 164.308, 164.310, 164.312, 164.314, and 164.316 with respect to EPHI.

2.6. **Breach of Unsecured PHI.** Business Associate shall report to Covered Entity without unreasonable delay, and within the timeframe required by applicable laws and regulations, any acquisition, access, use or disclosure of Unsecured Protected Health Information not permitted by this BAA. Such notification shall include an assessment of whether the incident constitutes a "Breach" under 45 CFR § 164.402. To the extent such assessment concludes that a Breach has occurred, or as requested by Covered Entity, such notification shall also include, to the extent possible, the identification of each Individual whose PHI has been or is reasonably believed to have been accessed, acquired, used or disclosed during the incident, along with any other information that the Covered Entity will be required to include in its notification to the Individual, the media and/or the Secretary, as applicable, including, without limitation, (a) a description of the incident, (b) the date of the incident and the date of its discovery, (c) the types of Unsecured Protected Health Information involved, and (d) a description of Business Associate's investigation, mitigation, and prevention efforts. In the event that a Breach occurs that is properly attributable to the acts or omissions of Business Associate, Business Associate shall cooperate and assist Covered Entity in preparing and, if so directed by Covered Entity, shall send any legally required written notifications. Breach Notification Rule.

2.7. **Security Incident.** Business Associate shall report to Covered Entity without unreasonable delay any Security Incident of which Business Associate becomes aware. Business Associate hereby reports to Covered Entity that incidents including, but not limited to, ping sweeps or other common network reconnaissance techniques, attempts to log on to a system with an invalid password or username, and denial of service attacks that do not result in a server being taken off line, may occur from time to time, are logged in the due course of business, and do not need to be further reported.

2.8. **Subcontractors.**

2.8.1. **Written Agreement.** Business Associate shall ensure that any Subcontractor that creates, receives, maintains or transmits PHI on its behalf agrees in writing to the same restrictions and conditions that apply to Business Associate with respect to such PHI.

2.8.2. **Violations of Agreement.** If Business Associate becomes aware of a pattern of activity or practice of a Subcontractor that constitutes a material violation of the Subcontractor's obligations under the written agreement described in Section 2.8.1 (Written Agreement),

Business Associate agrees to take reasonable steps to cure or end the violation, and if such steps are unsuccessful, to terminate the agreement, if feasible.

2.9. Individual Rights.

2.9.1. Request to Access or Amend PHI.

2.9.1.1. Individual Request to PHI. If any Individual submits a request to Business Associate for access to or amendment of his or her PHI in a Designated Record Set, Business Associate agrees to notify Covered Entity of such request so that Covered Entity may respond to the request in accordance with the requirements of 45 CFR §§ 164.524 and 164.526.

2.9.1.2. Covered Entity Request to PHI. If Covered Entity submits a request to Business Associate for access to or amendment of PHI in a Designated Record Set, Business Associate agrees to provide access and/or amend such PHI as directed in writing by Covered Entity, in accordance with the requirements of 45 CFR §§ 164.524 and 164.526.

2.9.1.3. Imposition of Cost for PHI Request. Business Associate may impose a reasonable cost-based fee on Covered Entity for the provision of access to PHI in a Designated Record Set in accordance with 45 CFR § 164.524(c)(4).

2.9.2. Request for Accounting of Disclosures.

2.9.2.1. Individual Request for Accounting. If any Individual submits a request to Business Associate for an accounting of disclosures of his or her PHI, Business Associate agrees to notify Covered Entity of such request.

2.9.2.2. Business Associate Request for Accounting. Business Associate agrees to provide to Covered Entity such information as is in Business Associate's possession and is necessary to enable Covered Entity to comply with the requirements of 45 CFR § 164.528 with respect to an Individual's request for an accounting of disclosures of PHI.

2.9.2.3. Appropriate Record Keeping. Business Associate agrees to implement an appropriate record keeping process to enable it to provide to Covered Entity such information as is required to be provided to an Individual in response to a request for an accounting of disclosures, as described at 45 CFR § 164.528.

2.10. Remuneration in Exchange for PHI. Except as permitted under 45 CFR § 164.502(a)(5)(ii), Business Associate agrees that it shall not directly or indirectly receive remuneration in exchange for PHI from or on behalf of the recipient of such PHI.

2.11. Audit. Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Business Associate from, Covered Entity in connection with the Services, available to the Secretary, upon request, for purposes of determining and facilitating Covered Entity's compliance with HIPAA.

2.12. Privacy Compliance. The parties do not anticipate that, in performing the Services, Business Associate will carry out Covered Entity's obligations under Subpart E of 45 C.F.R. Part 164. However, to the extent, in performing the Services, Business Associate is to carry out one or more of Covered Entity's obligations under Subpart E, Business Associate agrees to comply with the requirements of Subpart E

that apply to Covered Entity in the performance of such obligations.

3. Covered Entity Obligations.

3.1. Notice of Privacy Practices. Covered Entity shall notify Business Associate of limitation(s) in its notice of privacy practices, to the extent such limitation affects Business Associate's permitted uses or disclosures of PHI.

3.2. Individual Permission. Covered Entity shall notify Business Associate of change(s) in, or revocation of, permission by an Individual to use or disclose PHI, to the extent such change(s) affect(s) Business Associate's permitted uses or disclosures of PHI. Covered Entity agrees to obtain any patient authorizations or consents that may be required under state or federal law or regulation in order to transmit PHI to Business Associate and to enable Business Associate and its Subcontractors and agents to use and disclose PHI as contemplated by this BAA, including consents and authorizations relating to mental health, HIV, substance abuse, and other particularly sensitive conditions.

3.3. Restrictions. Covered Entity shall notify Business Associate of restriction(s) on the use or disclosure of PHI to which Covered Entity has agreed, to the extent such restriction(s) affect(s) Business Associate's permitted uses or disclosures of PHI.

3.4. Authorizations. Covered Entity is required to comply with state laws and HIPAA and obtain any required authorization for disclosure to the Business Associate.

4. Term & Termination.

4.1. Term. The term of this BAA shall begin on the Effective Date, and shall terminate when all PHI provided by Covered Entity to Business Associate, or created or received by Business Associate in connection with the Services provided with respect to patients of Covered Entity, is returned to Covered Entity or destroyed, as agreed by a duly authorized representative of Covered Entity in writing. For the avoidance of doubt, the return or destruction of PHI includes all PHI provided by Business Associate to any Subcontractor or created or received by a Subcontractor on behalf of Business Associate.

4.2. Termination for Cause.

4.2.1. By Covered Entity. Upon Covered Entity's knowledge of a material violation by Business Associate of this BAA, Covered Entity may:

4.2.1.1. Immediate Termination of Business Associate. Immediately terminate this BAA and the Services if Business Associate has violated a material term of this BAA and cure is not possible; or

4.2.1.2. Material Violation by Business Associate. Terminate this BAA and the Services if Covered Entity determines that Business Associate has violated a material term of this BAA if, following Covered Entity's notification to Business Associate of the material violation, Business Associate is unable or unwilling to take steps to cure the violation within such thirty (30) day period. In the event of such a cure, this BAA shall remain in full force and effect.

4.2.2. By Business Associate. Upon Business Associate's knowledge of a material violation by Covered Entity of this BAA, Business Associate may:

4.2.2.1. Immediate Termination of Covered Entity. Immediately terminate this BAA and the Services if Covered Entity has violated a material term of this BAA and cure is not possible; or

4.2.2.2. Material Violation by Covered Entity. Terminate this BAA and the Services upon thirty (30) days' notice, after (1) Business Associate determines that Covered Entity has violated a material term of this BAA, and (2) following Business Associate's written notification of the material violation to Covered Entity, Covered Entity is unable or unwilling to take steps to cure the violation within such thirty (30) day period. In the event Covered Entity cures the violation within such thirty (30) day period, this BAA shall remain in full force and effect.

4.3. Return or Destruction/Survival.

4.3.1. Effect of Termination. In the event of termination of this BAA pursuant to Section 4.2 (Termination for Cause), to the extent feasible, Business Associate shall return to Covered Entity or destroy all PHI that Business Associate still maintains in any form. For the avoidance of doubt, the return or destruction of PHI includes all PHI provided by Business Associate to any Subcontractor or created or received by a Subcontractor on behalf of Business Associate. If the return or destruction of all PHI is not feasible, Business Associate shall extend the protections of this BAA to the remaining information and limit further use and disclosure of PHI to those purposes that make the return or destruction of the PHI infeasible.

4.3.2. Survival. The terms of: (i) Section 2.6 (Breach of Unsecured PHI); (ii) Section 2.9.2 (Request for Accounting of Disclosures); and (iii) Section 2.11 (Audit).

5. Compliance with Laws. Business Associate and Covered Entity shall comply with all applicable federal, state and local laws, rules and regulations concerning the privacy and security of PHI, including, without limitation, the requirements of HIPAA, the HITECH Act, and GINA.

6. No Third-Party Beneficiaries. Nothing express or implied in this BAA is intended to confer, nor shall anything herein confer, upon any person other than the Covered Entity, Business Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

7. Amendment. The parties acknowledge that the Secretary may promulgate additional regulations and interpretative guidance that is not available at the time of executing this BAA. In the event Covered Entity or Business Associate determines in good faith that any such regulation or guidance adopted or amended after the execution of this BAA is required by law to be implemented and made a part hereof, this BAA shall be renegotiated in good faith so as to amend the applicable provision(s) in a manner that would eliminate any such substantial risk.

HIPAA BUSINESS ASSOCIATE AGREEMENT SIGNATURE PAGE

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement, and the same shall become effective as of the latest date of signature set forth below.

Covered Entity:	Business Associate: **Johnson & Johnson Vision Care, Inc.**
By: _____	By:  _____
Print name: _____	Print name: **Sherri Ferstler** _____
Title: _____	Title: **VP Sales USA** _____
Date: _____	Date: **March 9, 2021** _____