

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (the "Agreement"), effective as of _____ (Effective Date), is entered into by and between: _____ (the Plan Sponsor), on behalf of _____ (the group health plan, hereinafter the "Covered Entity") and GBS Benefits and its affiliates (the "Business Associate").

RECITALS

Whereas, the purpose of this Agreement is to comply with applicable requirements of the Health Insurance Portability and Accountability Act of 1996 and amendments thereto and regulations thereunder (hereinafter collectively referred to as "HIPAA Rules" and defined as the Privacy, Security, Breach Notification and Enforcement Rules at 45 CFR Part 160 and Part 164); and including amendments by (and regulations under) the "Health Information Technology for Economic and Clinical Health Act" ("HITECH Act") and by section 105 of Title I of the Genetic Information Nondiscrimination Act of 2008 ("GINA");

Whereas, Covered Entity and Business Associate have entered into, or may enter into, one or more agreements or arrangements under which Business Associate shall or may provide services to Covered Entity and may have access to, create and/or receive Protected Health Information in the performance of such services, or for or on behalf of Covered Entity;

Whereas, HIPAA allows a Covered Entity to disclose Protected Health Information to a Business Associate only pursuant to a Business Associate Agreement which provides satisfactory assurances that the Business Associate will appropriately safeguard the Protected Health Information;

Now, Therefore, in consideration of the parties' continuing obligations under this Agreement, compliance with HIPAA Privacy and Security rules, and other good and valuable consideration (the receipt of which is hereby acknowledged), the parties listed above hereby agree to the provisions of this Agreement in order to comply with the HIPAA requirements and to protect the interests of both parties.

1. DEFINITIONS

1.1 **Breach.** "Breach" shall have the same meaning as the term "breach" in 45 CFR §164.402, which is the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted, unless the Covered Entity demonstrates that there is a low probability the PHI has been compromised. The definition of Breach excludes the following uses and disclosures:

- (a) Unintentional access by a Covered Entity or Business Associate acting in good faith and within an employee's course and scope of employment;

- (b) Inadvertent one-time disclosure between Covered Entity or Business Associate work force members (including employee, volunteer, trainees, etc. whether paid or unpaid); and
- (c) The 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 the information.

For purposes of the HITECH requirements to notify Individuals of Breaches of PHI, a "Breach" will not be deemed to have occurred if the data accessed or disclosed is encrypted or otherwise secured using a technology or methodology specified by the Secretary of HHS which renders the data unusable, unreadable, or indecipherable to unauthorized individuals who access it.

- 1.2 **Breach Notification Rule.** "Breach Notification Rule" shall mean the Standards and Implementation Specifications for Notification of Breaches of Unsecured Protected Health Information under 45 CFR Parts 160 and 164, subparts A and D.
- 1.3 **Business Associate.** "Business Associate" shall have the same meaning as the term "business associate" at 45 CFR §160.103, and is the entity named as Business Associate in the opening paragraph of this Agreement. Generally, a Business Associate is a person who, on behalf of a Covered Entity (and not as a member of the Covered Entity's workforce):
 - (a) performs (or assists in the performance of) a function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management and repricing; or any other function or activity regulated by 45 CFR Part 160; or
 - (b) provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services to or for a Covered Entity.
- 1.4 **Covered Entity.** "Covered Entity" shall have the same meaning as the term "covered entity" at 45 CFR §160.103, and in reference to the party to this agreement, shall mean the entity named as Covered Entity in the opening paragraph of this Agreement. Generally, a Covered Entity may be a health plan, health care clearinghouse, or health care provider who transmits any health information in electronic form in connection with a transaction covered by 45 CFR Part 160.
- 1.5 **Electronic Protected Health Information or ePHI.** "Electronic Protected Health Information" or "ePHI" shall have the same meaning as the term "electronic protected health information" in 45 CFR §160.103, which is individually identifiable Protected Health Information that is maintained in or transmitted by electronic media.
- 1.6 **Electronic Transactions Rule.** "Electronic Transactions Rule" shall mean the final regulations issued by HHS concerning standard transactions and code sets under 45 CFR Parts 160 and 162.
- 1.7 **Genetic Information.** "Genetic Information" shall have the same meaning as the term "genetic information" in 45 CFR §160.103.
- 1.8 **HHS.** "HHS" shall mean the Department of Health and Human Services.
- 1.9 **HIPAA Rules.** "HIPAA Rules" shall mean the Privacy Rule, Security Rule, Breach Notification Rule, and Enforcement Rule.

- 1.10 **HITECH Act.** "HITECH Act" shall mean the Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009.
- 1.11 **Privacy Rule.** "Privacy Rule" shall mean the Privacy Standards and Implementation Specifications at 45 CFR Part 160 and 45 CFR Part 164, subparts A and E.
- 1.12 **Protected Health Information or PHI.** "Protected Health Information" or "PHI" shall have the same meaning as the term "protected health information" in 45 CFR §160.103, which is any individually identifiable health information, whether oral or recorded in any form or medium:
- (a) that is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
 - (b) that relates to the past, present, or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and
 - (c) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
 - (d) Except that PHI excludes employment records held by the Covered Entity in its role as employer.
- For purposes of this Agreement, the term shall be limited to PHI created or received by Business Associate (or a Subcontractor) from or on behalf of Covered Entity.
- 1.13 **Required by Law.** "Required by Law" shall have the same meaning as the term "required by law" in 45 CFR §164.103.
- 1.14 **Security Incident.** "Security Incident" shall have the same meaning as the term "security incident" in 45 CFR §164.304, which is the unauthorized access to, use, disclosure, modification or destruction of, or interference with, Electronic Protected Health Information (ePHI) or interference with system operations in an information system containing ePHI.
- 1.15 **Security Rule.** "Security Rule" shall mean the Security Standards and Implementation Specifications at 45 CFR Part 160 and 45 CFR Part 164, subparts A and C.
- 1.16 **Subcontractor.** "Subcontractor" shall have the same meaning as the term "subcontractor" in 45 CFR §160.103.
- 1.17 **Unsecured Protected Health Information or PHI.** "Unsecured Protected Health Information or PHI" shall have the meaning given the term "unsecured protected health information" in 45 CFR §164.402, which is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals using a technology or methodology specified by the Secretary of HHS.

II. Privacy and Security of Protected Health Information

2.1 **Permitted Uses and Disclosures.** Business Associate is permitted to use and disclose Protected Health

Information only as set forth below:

- 2.1.1 **Functions and Activities on Covered Entity's Behalf.** Business Associate may use and disclose Protected Health Information to provide services to the Covered Entity. The specific services may be listed in a service agreement, broker of record letter or by other written or verbal agreement. Business Associate is authorized to use Protected Health Information to de-identify it and to use or disclose the de-identified information as agreed to by the parties.
- 2.1.2 **Business Associate's Operations.** Business Associate may use or disclose Protected Health Information for the proper management and administration of Business Associate or to carry out the legal responsibilities of the Business Associate, provided that, for any *disclosure* of PHI:
- (A) The disclosure is Required by Law; or
 - (B) Business Associate obtains reasonable assurance from any person or entity to which Business Associate will disclose Protected Health Information that the person or entity will:
 - (1) Hold the Protected Health Information in confidence and use or further disclose the Protected Health Information only for the purpose for which Business Associate disclosed Protected Health Information to the person or entity or as Required by Law; and
 - (2) Promptly notify Business Associate of any instance of which the person or entity becomes aware in which the confidentiality of Protected Health Information was breached.
- 2.2 **Minimum Necessary.** Business Associate will, in its performance of the functions, activities, services, and operations specified above, make reasonable efforts to use, to disclose, and to request only the minimum amount of Protected Health Information reasonably necessary to accomplish the intended purpose of the use, disclosure, or request, except that Business Associate will not be obligated to comply with this minimum-necessary limitation if neither Business Associate nor Covered Entity is required to limit its use, disclosure, or request to the minimum necessary under the HIPAA Rules. Business Associate and Covered Entity acknowledge that the phrase "minimum necessary" shall be interpreted in accordance with the HITECH Act and the HIPAA Rules.
- 2.3 **Prohibition on Unauthorized Use or Disclosure.** Business Associate will neither use nor disclose Protected Health Information, except as permitted or required by this Agreement or in writing by Covered Entity or as Required by Law. This Agreement does not authorize Business Associate to use or disclose Covered Entity's Protected Health Information in a manner that would violate the HIPAA Rules if done by Covered Entity, except as permitted for Business Associate's proper management and administration, as described above.
- 2.4 Information Safeguards.**
- 2.4.1 **Privacy of Protected Health Information.** Business Associate will develop, implement, maintain, and use appropriate administrative, technical, and physical safeguards to protect the privacy of Protected Health Information. The safeguards must reasonably protect Protected Health Information from any intentional or unintentional use or disclosure in violation of the Privacy Rule

and limit incidental uses or disclosures made pursuant to a use or disclosure otherwise permitted by this Agreement. To the extent the parties agree that the Business Associate will carry out directly one or more of Covered Entity's obligations under the Privacy Rule, the Business Associate will comply with the requirements of the Privacy Rule that apply to the Covered Entity in the performance of such obligations.

2.4.2 Security of Covered Entity's Electronic Protected Health Information. Business Associate will comply with the Security Rule and will use appropriate administrative, technical, and physical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic Protected Health Information that Business Associate creates, receives, maintains, or transmits on Covered Entity's behalf. Business Associate will identify and protect against reasonably anticipated impermissible uses or disclosures of – or threats to the security or integrity of -- Covered Entity's Electronic Protected Health Information.

2.5 Subcontractors. Business Associate will require each of its Subcontractors to agree, in a written agreement with Business Associate, to comply with the provisions of the Security Rule; to appropriately safeguard Protected Health Information created, received, maintained, or transmitted on behalf of the Business Associate; and to apply the same restrictions and conditions that apply to the Business Associate with respect to such Protected Health Information. If a Subcontractor violates such restrictions or conditions, Business Associate will impose appropriate sanctions against the Subcontractor and will mitigate the effects of any such violations.

2.6 Prohibition on Sale of Protected Health Information. Business Associate shall not sell Covered Entity's Protected Health Information (as defined in the HIPAA rules), nor use it for marketing purposes.

2.7 Prohibition on Use or Disclosure of Genetic Information. Business Associate shall not use or disclose Genetic Information for underwriting purposes in violation of the HIPAA rules.

2.8 Penalties for Noncompliance. Business Associate acknowledges that it is subject to civil and criminal enforcement for failure to comply with the HIPAA Rules, to the extent provided by the HITECH Act and the HIPAA Rules.

III. Compliance with Electronic Transactions Rule.

If Business Associate conducts in whole or part electronic Transactions on behalf of Covered Entity for which HHS has established standards, Business Associate will comply, and will require any Subcontractor it involves with the conduct of such Transactions to comply, with each applicable requirement of the Electronic Transactions Rule and of any operating rules adopted by HHS with respect to Transactions.

IV. Individual Rights.

4.1 Access. Business Associate will, within fifteen (15) calendar days following Covered Entity's request, make available to Covered Entity (or, at Covered Entity's written direction, to an individual or the individual's designee) for inspection and copying Protected Health Information about the individual that

is in a Designated Record Set in Business Associate's custody or control, so that Covered Entity may meet its access obligations under 45 CFR §164.524 (which provides for 30 days). If Covered Entity requests an electronic copy of Protected Health Information that is maintained electronically in a Designated Record Set in the Business Associate's custody or control, Business Associate will provide an electronic copy in the form and format specified by the Covered Entity if it is readily producible in such format; if it is not readily producible in such format, Business Associate will work with Covered Entity to determine an alternative form and format that enable Covered Entity to meet its electronic access obligations under 45 CFR §164.524.

- 4.2 **Amendment.** Business Associate will, upon receipt of written notice from Covered Entity, promptly amend or permit Covered Entity access to amend any portion of an individual's Protected Health Information that is in a Designated Record Set in the custody or control of the Business Associate, so that Covered Entity may meet its amendment obligations under 45 CFR §164.526.
- 4.3 **Disclosure Accounting.** To allow Covered Entity to meet its obligations to account for disclosures of Protected Health Information under 45 CFR §164.528, Business Associate will record the "Disclosure Information" specified below for each disclosure of Protected Health Information that Business Associate makes to Covered Entity or to a third party, except that Business Associate will not be obligated to record Disclosure Information or otherwise account for disclosures of Protected Health Information if Covered Entity need not account for such disclosures under the HIPAA Rules.
- 4.4 **Disclosure Information.** Business Associate will record the following information if required:
- (A) For non-repetitive disclosures: (i) the disclosure date, (ii) the name and (if known) address of the entity to which Business Associate made the disclosure, (iii) a brief description of the Protected Health Information disclosed, and (iv) a brief statement of the purpose of the disclosure.
 - (B) For repetitive disclosures (made for a single purpose to the same person or entity, including to Covered Entity): (i) the Disclosure Information specified above for the first of the repetitive accountable disclosures; (ii) the frequency, periodicity, or number of the repetitive accountable disclosures; and (iii) the date of the last of the repetitive accountable disclosures.
- 4.5 **Availability of Disclosure Information.** Business Associate will maintain the Disclosure Information for at least 6 years following the date of the accountable disclosure to which the Disclosure Information relates. Business Associate will make the Disclosure Information available to Covered Entity within thirty (30) calendar days following Covered Entity's request for such Disclosure Information to comply with an individual's request for disclosure accounting. [*Covered Entity has up to 60 days to provide accounting to an individual.*]
- 4.6 **Restriction Agreements and Confidential Communications.** Covered Entity shall notify Business Associate of any limitations in the notice of privacy practices of Covered Entity under 45 CFR §164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information. Business Associate will comply with any notice from Covered Entity to (1) restrict use or disclosure of Protected Health Information pursuant to 45 CFR §164.522(a), or (2) provide for

confidential communications of Protected Health Information pursuant to 45 CFR §164.522(b), provided that Covered Entity notifies Business Associate in writing of the restriction or confidential communications obligations that Business Associate must follow. Covered Entity will promptly notify Business Associate in writing of the termination of any such restriction or confidential communications requirement and, with respect to termination of any such restriction, instruct Business Associate whether any of the Protected Health Information will remain subject to the terms of the restriction agreement.

V. Breaches and Security Incidents.

5.1 Reporting.

- 5.1.1 **Impermissible Use or Disclosure.** Business Associate will report to Covered Entity any use or disclosure of Protected Health Information not permitted by this Agreement not more than fifteen (15) calendar days after Business Associate discovers such non-permitted use or disclosure.
- 5.1.2 **Breach of Unsecured Protected Health Information.** Business Associate will report to Covered Entity any Breach of Unsecured Protected Health Information impacting the Plan not more than fifteen (15) calendar days after discovery of such Breach. Covered Entity then has sixty (60) days to provide required notifications to individuals if a breach occurred, and, in appropriate cases, to the media and HHS. Business Associate will treat a Breach as being discovered in accordance with 45 CFR §164.410. Business Associate will make the report to Covered Entity's Privacy Officer. If a delay is requested by a law-enforcement official in accordance with 45 CFR §164.412, Business Associate may delay notifying Covered Entity for the applicable time period. Business Associate's report will include at least the following, where absence of any information will not be cause for Business Associate to delay the report:
- (A) Identify the nature of the Breach, which will include a brief description of what happened, including the date of any Breach and the date of the discovery of any Breach;
 - (B) Identify the types of Protected Health Information that were involved in the Breach (e.g., name, Social Security number, date of birth, home address, account number, diagnosis);
 - (C) Identify who made the non-permitted use or disclosure and who received it;
 - (D) Identify what corrective or investigational action Business Associate took or will take to prevent further non-permitted uses or disclosures, to mitigate harmful effects, and to protect against any further Breaches;
 - (E) Identify what steps the individuals who were subject to a Breach should take to protect themselves;
 - (F) Provide such other information, including a written report and risk assessment under 45 CFR §164.402, as Covered Entity may reasonably request.
- 5.1.3 **Security Incidents.** Business Associate will report to Covered Entity any Security Incident of which

Business Associate becomes aware where the Covered Entity may be affected. Business Associate will make this report annually, except if any such Security Incident resulted in a disclosure not permitted by this Agreement or Breach of Unsecured Protected Health Information, Business Associate will make the report in accordance with the provisions set forth above.

Although the following technically *are* security incidents, these and other trivial, unsuccessful attempts to bypass BA's or subcontractor's security system need NOT be reported to CE: any unsuccessful attempt to bypass Business Associate's (or a Subcontractor's) security system including, but not limited to, pings, password-based attacks, unsuccessful log-on attempts and other common attacks on Business Associate's (or a Subcontractor's) firewall, as long as such incident does not result in unauthorized use or disclosure of ePHI or significantly compromise Business Associate's (or a Subcontractor's) security safeguards.

5.2 **Mitigation.** Business Associate shall mitigate, to the extent practicable, any harmful effect known to the Business Associate resulting from a use or disclosure in violation of this Agreement.

5.3 **Breach Notification to Third Parties.** Covered Entity is responsible to notify third parties if a breach of Unsecured Protected Health Information occurs. Business Associate will notify Covered Entity as provided above.

VI. Term and Termination.

6.1 **Term.** This Agreement shall be effective as of the Effective Date specified above in the first paragraph, and shall terminate upon termination of the underlying services agreement or Broker of Record letter between Business Associate and plan sponsor of the Covered Entity, subject to the provisions regarding return or destruction of PHI (in section 6.3 below).

6.2 **Right to Terminate for Cause.** If Covered Entity determines that Business Associate has breached a material provision of this Agreement, it may terminate this Agreement if it provides written notice to Business Associate of the alleged breach and gives Business Associate an opportunity to cure the breach. Any such termination will be effective immediately or at such other date specified in Covered Entity's notice of termination. If neither termination nor cure is feasible, Covered Entity shall report the breach to the Secretary of HHS.

6.3 Treatment of Protected Health Information on Termination.

6.3.1 **If Return or Destruction of Covered Entity's Protected Health Information Is Feasible.** Upon termination of this Agreement, Business Associate will, if feasible, return to Covered Entity or destroy all Protected Health Information in whatever form or medium, including all copies thereof and all data derived therefrom that allow identification of any individual who is a subject of the Protected Health Information. This provision shall apply to Protected Health Information that is in the possession of any Subcontractors of Business Associate. Further, Business Associate shall require any such Subcontractor to certify to Business Associate that it has returned or destroyed all

such information which could be returned or destroyed. Business Associate will complete these obligations as promptly as possible.

- 6.3.2 Procedure When Return or Destruction Is Not Feasible.** Business Associate will identify any Protected Health Information, including any Protected Health Information that Business Associate has disclosed to Subcontractors, that cannot feasibly be returned to Covered Entity or destroyed and explain why return or destruction is infeasible. Business Associate will require all Subcontractors to return any such Protected Health Information to Business Associate and will limit its further use or disclosure of such information to those purposes that make return or destruction of such information infeasible. Business Associate will complete these obligations as promptly as possible.
- 6.3.3 Continuing Privacy and Security Obligation.** Business Associate's obligation to protect the privacy and safeguard the security of Protected Health Information as specified in this Agreement will be continuous and survive termination or other conclusion of this Agreement.

VII. General Provisions.

- 7.1 Definitions.** All terms that are used but not otherwise defined in this Agreement shall have the meaning specified under HIPAA, including its statute, regulations, and other official government guidance.
- 7.2 Inspection of Internal Practices, Books, and Records.** Business Associate will make its internal practices, books, and records relating to its use and disclosure of PHI and ePHI available to Covered Entity and to HHS to determine compliance with the HIPAA Rules.
- 7.3 Amendment to Agreement.** This Agreement may be amended only by a written instrument signed by the parties, except that if there is a change in applicable law or guidance and the parties have not timely adopted an appropriate amendment, this Agreement shall be amended automatically and deemed to incorporate such new or revised provisions as are necessary to comply with the change in the law or guidance. The parties agree to negotiate in good faith to adopt such amendments as are necessary to comply with changes in the law or guidance.
- 7.4 No Third-Party Beneficiaries.** Nothing in this Agreement shall be construed as creating any rights or benefits to any third parties.
- 7.5 Interpretation.** Any ambiguity in the Agreement shall be resolved to permit Covered Entity and Business Associate to comply with the applicable requirements under the HIPAA Rules.
- 7.6 Indemnification.**

Business Associate agrees to defend, indemnify, and hold harmless Covered Entity, its officers, agents, and employees from and against any and all claims, liabilities, demands, damages, losses, costs, and

expenses (including costs and reasonable attorney's fees) arising from a Breach by Business Associate, its officers, agents or employees, of Business Associate's obligations under this Agreement.

Covered Entity agrees to defend, indemnify, and hold harmless Business Associate, its officers, agents, and employees from and against any and all claims, liabilities, demands, damages, losses, costs, and expenses (including costs and reasonable attorney's fees) arising from a Breach by Covered Entity, its officers, agents or employees, of Covered Entity's obligations under this Agreement.

7.7 **Severability.** The invalidity or unenforceability of any provisions of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement, which shall remain in full force and effect.

7.8 **Construction and Interpretation.** The section headings contained in this Agreement are for reference purposes only and shall not in any way affect the meaning or interpretation of this Agreement. This Agreement has been negotiated by the parties at arm's-length and each of them has had an opportunity to modify the language of the Agreement. Accordingly, the Agreement shall be treated as having been drafted equally by the parties, and the language shall be construed as a whole and according to its fair meaning. Any presumption or principle that the language is to be construed against any party shall not apply. This Agreement may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement.

7.9 **Notices.** All notices and communications required by this Agreement shall be in writing. Such notices and communications shall be given in one of the following forms: (a) by delivery in person, (b) by a nationally-recognized, next-day courier service, (c) by first-class, registered or certified mail, postage prepaid; or (d) by electronic mail to the address that each party specifies in writing.


7.10 **Entire Agreement.** This Agreement constitutes the entire agreement between the parties with respect to its subject matter and constitutes and supersedes all prior agreements, representations and understandings of the parties, written or oral, with regard to this same subject matter.

In Witness Whereof, the Parties hereto have duly executed this Agreement as of the Effective Date as defined in the initial paragraph.

Plan Sponsor _____
on behalf of the _____

Signature _____
Printed Name _____
Title _____
Date _____

Business Associate GBS Benefits and its affiliates
(Must be signed by an officer permitted to contract with Plan)

Signature 
Printed Name Matt Kiisel
Title Senior Vice President of Operations
Date _____