ATTACHMENT 3
DRAFT BUSINESS ASSOCIATE AGREEMENT

Washington State Health Care Authority	**BUSINESS ASSOCIATE AGREEMENT**	HCA Contract Number: KXXX Business Associate Contract Number:

THIS BUSINESS ASSOCIATE AGREEMENT made by and between Washington State Health Care Authority, hereinafter referred to as "HCA," and the party whose name appears below, hereinafter referred to as the "Business Associate."

BUSINESS ASSOCIATE NAME	BUSINESS ASSOCIATE doing business as (DBA)
BUSINESS ASSOCIATE ADDRESS **[Street]** **[City], [ST] [Zip Code]**	BUSINESS ASSOCIATE CONTACT
BUSINESS ASSOCIATE CONTACT TELEPHONE ( ) -	BUSINESS ASSOCIATE CONTACT E-MAIL ADDRESS **[Email Address]**

HCA PROGRAM **[Enter Program Name]**	HCA DIVISION/SECTION
HCA CONTACT NAME AND TITLE **[Name]** **[Title]**	HCA CONTACT ADDRESS **Cherry Street Plaza** **626 8th Avenue SE** **Olympia, WA 98504-____**
HCA CONTACT TELEPHONE ( ) -	HCA CONTACT E-MAIL ADDRESS **[Email Address]**

This terms and conditions of this Business Associate Agreement are an integration and representation of the final, entire and exclusive understanding between the parties superseding and merging all previous agreements, writings, and communications, oral or otherwise, regarding the subject matter of this Business Associate Agreement. The parties signing below warrant that they have read and understand this Business Associate Agreement, and have authority to execute this Business Associate Agreement. This Business Associate Agreement shall be binding on HCA only upon signature by HCA.

BUSINESS ASSOCIATE SIGNATURE	PRINTED NAME AND TITLE	DATE SIGNED
HCA SIGNATURE	PRINTED NAME AND TITLE	DATE SIGNED

TABLE OF CONTENTS

This BUSINESS ASSOCIATE AGREEMENT is made between [**ENTER BUSINESS ASSOCIATE NAME**] (Business Associate) and the Washington State Health Care Authority (HCA). This agreement does not expire or automatically terminate except as stated in Section 5.

This Agreement relates to all business relationships between the Business Associate and HCA unless otherwise agreed. Business Associate is or may be a "Business Associate" of HCA as defined in the HIPAA Rules. If there is a conflict between the provisions of this Agreement and provisions of other contracts, this Agreement controls; otherwise, the provisions in this Agreement do not replace any provisions of any other contracts. If the other Contract is terminated, this Agreement nonetheless continues in effect.

This Business Associate Agreement supersedes any existing Business Associate Agreement the Business Associate may have with HCA. It also supersedes any "business associate" section in an underlying Contract.

1 Definitions

1.1 Access attempts

Information systems are the frequent target of probes, scans, "pings," and other activities that may or may not indicate threats, whose sources may be difficult or impossible to identify, and whose motives are unknown, and which do not result in access or risk to any information system or PHI. Those activities are "access attempts."

1.2 Day

"Day" means business days observed by Washington State government.

1.3 Catch-all definitions

The following terms used in this Agreement have the same meaning as those terms in the HIPAA Rules: Breach, Business Associate, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information (PHI), and Use.

1.4 Clients or Individuals

"Clients" or "individuals" are people who have health or other coverage or benefits from or through HCA. They include Medicaid clients, Public Employees Benefits Board subscribers and enrollees, and others.

1.5 Contract or Underlying Contract

"Contract" or "underlying contract" means all agreements between Business Associate and HCA under which Business Associate is a "business associate" as defined in the Security or Privacy Rules. The terms apply whether there is one such agreement or more than one, and if there is more than one the terms include them all even though a singular form is used except as otherwise specified. The terms include agreements now in effect and agreements that become effective after the effective date of this Agreement.

1.6 Effective Date

"Effective Date" means the date of the signature with the latest date affixed to the Agreement.

1.7 HIPAA Rules; Security, Breach Notification, and Privacy Rules

"HIPAA Rules" means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164, as now in effect and as modified from time to time. In part 164 of title 45 CFR, the "Security Rule" is subpart C (beginning with §164.302), the "Breach Notification Rule" is subpart D (beginning with § 164.400), and the "Privacy Rule" is subpart E (beginning with § 164.500).

1.8 Protected Health Information or PHI

"Protected Health Information" has the same meaning as in the HIPAA Rules except that in this Agreement the term includes only information created by Business Associate or any of its contractors, or received from or on behalf of HCA, and relating to Clients. "PHI" means Protected Health Information.

2 Obligations and Activities of Business Associate

2.1 Limits

Business Associate will not use or disclose PHI other than as permitted or required by the Contract or this Agreement or as required by law. Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI on behalf of, or as necessary for purposes of the underlying contract, if such use or disclosure of PHI would not violate the Privacy Rule if done by a Covered Entity and is the minimum necessary.

2.2 Safeguards

Business Associate will use appropriate safeguards, and will comply with the Security Rule with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for by the Contract or this Agreement. Business Associate will store and transfer PHI in encrypted form.

2.3 Reporting Security Incidents

2.3.1 Business Associate will report security incidents that materially interfere with an information system used in connection with PHI. Business Associate will report those security incidents to HCA within five days of their discovery by Business Associate. If such an incident is also a Breach or may be a Breach, subsection 2.4 applies instead of this provision.

2.3.2 Access Attempts shall be recorded in Business Associate's system logs. Access Attempts are not categorically considered unauthorized Use or Disclosure, but Access Attempts do fall under the definition of Security Incident and Business Associate is required to report them to HCA.

Since Business Associate's reporting and HCA's review of all records of Access

Attempts would be materially burdensome to both parties without necessarily reducing risks to information systems or PHI, the parties agree that Business Associate will review logs and other records of Access Attempts, will investigate events where it is not clear whether or not an apparent Access Attempt was successful, and determine whether an Access Attempt:

a. Was in fact a "successful" unauthorized Access to, or unauthorized Use, Disclosure, modification, or destruction of PHI subject to this Agreement, or

b. Resulted in material interference with Business Associate's information system used with respect to PHI subject to this Agreement, or

c. Caused an unauthorized Use or Disclosure.

2.3.3 Subject to Business Associate's performance as described in 2.3.2., this provision shall serve as Business Associate's notice to HCA that Access Attempts will occur and are anticipated to continue occurring with respect to Business Associate's information systems. HCA acknowledges this notification, and Business Associate is not required to provide further notification of Access Attempts unless they are successful as described in Section 2.3.2. above, in which case Business Associate will report them in accordance with Section 2.3.1 or Section 2.4.

2.4 Breach notification

2.4.1 "Breach" is defined in the Breach Notification Rule. The time when a Breach is considered to have been discovered is explained in that Rule. HCA, or its designee, is responsible for determining whether an unauthorized Use or Disclosure constitutes a Breach under the Breach Notification Rule, and for any notification under the Breach Notification Rule.

2.4.2 Business Associate will notify HCA of any unauthorized use or disclosure and any other possible Breach within five days of discovery. If Business Associate does not have full details at that time, it will report what information it has, and provide full details within 15 days after discovery. The initial report may be oral. Business Associate will give a written report to HCA, however, as soon as possible. To the extent possible, these reports must include the following:

a. The identification of each individual whose PHI has been or may have been accessed, acquired, or disclosed;

b. The nature of the unauthorized Use or Disclosure, including a brief description of what happened, the date of the event(s), and the date of discovery;

c. A description of the types of PHI involved;

d. The investigative and remedial actions the Business Associate or its subcontractor took or will take to prevent and mitigate harmful effects, and protect against recurrence;

e. Any details necessary for a determination of the potential harm to Individuals whose PHI is believed to have been Used or Disclosed and the steps such Individuals should take to protect themselves; and

f. Such other information as HCA may reasonably request.

2.4.3 If Business Associate determines that it has or may have an independent notification obligation under any state breach notification laws, Business Associate will promptly notify HCA. In any event, Business Associate will notify HCA of its intent to give any notification under a state breach notification law no fewer than ten business days before giving such notification.

2.4.4 If Business Associate or any subcontractor or agent of Business Associate actually makes or causes, or fails to prevent, a use or disclosure constituting a Breach within the meaning of the Breach Notification Rule, and if notification of that use or disclosure must (in the judgment of HCA) be made under the Breach Notification Rule, or RCW 42.56.590 or RCW 19.254.010, or other law or rule, then:

a. HCA may choose to make any notifications to the individuals, to the Secretary, and to the media, or direct Business Associate to make them or any of them.

b. In any case, Business Associate will pay the reasonable costs of notification to individuals, media, and governmental agencies and of other actions HCA reasonably considers appropriate to protect clients (such as paying for regular credit watches in some cases), and

c. Business Associate will compensate HCA clients for harms caused to them by the Breach or possible Breach described above.

2.4.5 Business Associate's obligations regarding breach notification survive the termination of this Agreement and continue for as long as Business Associate maintains the PHI and for any breach or possible breach at any time.

2.5 Subcontractors

Business Associate will ensure that any subcontractors or agents that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to protective restrictions, conditions, and requirements at least as strict as those that apply to the Business Associate with respect to that information. Upon request by HCA, Business Associate will identify to HCA all its subcontractors and provide copies of its agreements (including business associate agreements or contracts) with them. The fact that Business Associate subcontracted or otherwise delegated any responsibility to a subcontractor or anyone else does not relieve Business Associate of its responsibilities.

2.6 Access

Business Associate will make available PHI in a designated record set to the HCA as necessary to satisfy HCA's obligations under 45 CFR § 164.524. Business Associate will give the information to HCA within five days of the request from the individual or HCA, whichever is earlier. If HCA requests, Business Associate will make that information

available directly to the individual. If Business Associate receives a request for access directly from the individual, Business Associate will inform HCA of the request within three days, and if requested by HCA it will provide the access in accordance with the HIPAA Rules.

2.7 Amending PHI

Business Associate will make any amendments to PHI in a designated record set as directed or agreed to by the HCA pursuant to 45 CFR § 164.526, or take other measures requested by HCA to satisfy HCA's obligations under that provision. If Business Associate receives a request for amendment directly from an individual, Business Associate will both acknowledge it and inform HCA within three days, and if HCA so requests act on it within ten days and inform HCA of its actions.

2.8 Accounting

Business Associate will maintain and make available to HCA the information required to provide an accounting of disclosures as necessary to satisfy HCA's obligations under 45 CFR § 164.528. If Business Associate receives an individual's request for an accounting, it will either provide the accounting as required by the Privacy Rule or, at its option, pass the request on to HCA within ten days after receiving it.

2.9 Obligations

To the extent the Business Associate is to carry out one or more of HCA's obligations under the Privacy Rule, it will comply with the requirements of that rule that apply to HCA in the performance of such obligations.

2.10 Books, etc.

Business Associate will make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

2.11 Mitigation

Business Associate will mitigate, to the extent practicable, any harmful effect of a use or disclosure of PHI by Business Associate or any of its agents or subcontractors in violation of the requirements of any of the HIPAA Rules, this Agreement, or the Contract.

2.12 Indemnification

To the fullest extent permitted by law, Business Associate will indemnify, defend, and hold harmless the State of Washington, HCA, and all officials, agents and employees of the State from and against all claims of any kind arising out of or resulting from the performance of this Agreement, including Breach or violation of HIPAA Rules.

3 Permitted Uses and Disclosures by Business Associate

3.1 Limited use and disclosure

Except as provided in this Section 3, Business Associate may use or disclose PHI only as necessary to perform the services set forth in the Contract.

3.2 General limitation

Business Associate will not use or disclose PHI in a manner that would violate the Privacy Rule if done by HCA.

3.3 Required by law

Business Associate may use or disclose PHI as Required by Law.

3.4 De-identifying

Business Associate may de-identified PHI in accordance with 45 CFR § 164.514(a)-(c).

3.5 Minimum necessary

Business Associate will make uses and disclosures of only the minimum necessary PHI, and will request only the minimum necessary PHI.

3.6 Disclosure for management and administration of Business Associate

3.6.1 Subject to subsection 3.6.2, Business Associate may disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of the Business Associate.

3.6.2 The disclosures mentioned in subsection 3.6.1 above are permitted only if either:

a. The disclosures are required by law, or

b. Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the 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 that the person will notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

3.7 Aggregation

Business Associate may use PHI to provide data aggregation services relating to the health care operations of the HCA, if those services are part of the Contract.

4 Activities of HCA

4.1 Notice of privacy practices

HCA will provide a copy of its current notice of privacy practices under the Privacy Rule to Business Associate on request. HCA will also provide any revised versions of that notice by posting on its website, and will send it on request.

4.2 Changes in permissions

HCA will notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

4.3 Restrictions

HCA will notify Business Associate of any restriction on the use or disclosure of PHI that HCA has agreed to or is required to abide by under 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI. Business Associate will comply with any such restriction.

5 Term and Termination

5.1 Term

5.1.1 This Agreement is effective as of the earliest of:

a. The first date on which Business Associate receives or creates PHI subject to this Agreement, or

b. The effective date of the Contract, or if there is more than one Contract then the effective date of the first one to be signed by both parties.

5.1.2 This Agreement continues in effect until the earlier of:

a. Termination of the provision of Services under the Contract or, if there is more than one Contract, under the last of the Contracts under which services are terminated,

b. The termination of this Agreement as provided below, or

c. The written agreement of the parties.

5.2 Termination for Cause

HCA may terminate this Agreement and the Contract (or either of them), if HCA determines Business Associate has violated a material term of the Agreement. The termination will be effective as of the date stated in the notice of termination.

5.3 Obligations of Business Associate upon termination

The obligations of the Business Associate under this subsection 5.3 survive the termination of the Agreement. Upon termination of this Agreement for any reason, Business Associate will:

5.3.1 Retain only that PHI that is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

5.3.2 Return to HCA or, if agreed to by HCA, destroy the PHI that the Business Associate and any subcontractor of Business Associate still has in any form (for purposes of this subsection 5.3, to destroy PHI is to render it unusable, unreadable, or indecipherable to the extent necessary to establish it is not Unsecured PHI, and Business Associate will provide HCA with appropriate evidence of destruction within ten days of the destruction);

5.3.3 Continue to use appropriate safeguards and comply with the Security Rule with respect to electronic PHI to prevent use or disclosure of the PHI, other than as provided for in this Agreement, for as long as Business Associate retains any of the PHI (for purposes of this subsection 5.3, If the PHI is destroyed it shall be rendered unusable, unreadable or indecipherable to the extent necessary to establish it is not Unsecured PHI. Business Associate will provide HCA with appropriate evidence of destruction);

5.3.4 Not use or disclose any PHI retained by Business Associate other than for the purposes for which the PHI was retained and subject to the same conditions that applied before termination;

5.3.5 Return to HCA, or, if agreed to by HCA, destroy, the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities; and

5.3.6 Business Associate's obligations relating to providing information to the Secretary and other government survive the termination of this Agreement for any reason.

5.4 Successor

Nothing in this Agreement limits the obligations of Business Associate under the Contract regarding giving data to HCA or to a successor Business Associate after termination of the Contract.

6 Miscellaneous

6.1 Amendment

The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

6.2 Interpretation

Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

6.3 HCA Contact for Reporting and Notification Requirements

Business Associate will address all reporting and notification communications required in this Agreement to:

HCA Privacy Officer
Washington State Health Care Authority
626 8th Avenue SE
PO Box 42700
Olympia, WA 98504-2700
Telephone: 360-725-1116
E-mail: PrivacyOfficer@hca.wa.gov