ATTACHMENT E: DATA USE, SECURITY AND CONFIDENTIALITY

1 Definitions

The definitions below apply to this Attachment:

1.1 **"Authorized User"** means an individual or individuals with an authorized business need to access HCA's Confidential Information under this Contract.

1.2 **"Breach"** means the unauthorized acquisition, access, use, or disclosure of Data shared under this Contract that compromises the security, confidentiality or integrity of the Data.

1.3 **"Business Associate"** means a Business Associate as defined in 45 CFR 160.103, who performs or assists in the performance of an activity for or on behalf of HCA, a Covered Entity that involves the use or disclosure of protected health information (PHI). Any reference to Business Associate in this DSA includes Business Associate's employees, agents, officers, Subcontractors, third party contractors, volunteers, or directors.

1.4 **Business Associate Agreement"** means the HIPAA Compliance section of this Exhibit and includes the Business Associate provisions required by the U.S. Department of Health and Human Services, Office for Civil Rights.

1.5 **"Covered Entity"** means HCA, which is a Covered Entity as defined in 45 C.F.R. § 160.103, in its conduct of covered functions by tis health care components.

1.6 **"Data"** means the information that is disclosed or exchanged as described by this Contract. For purposes of this Attachment, Data means the same as "Confidential Information."

1.7 **"Designated Record Set"** means a group of records maintained by or for a Covered Entity, that is: the medical and billing records about Individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or Used in whole or part by or for the Covered Entity to make decisions about Individuals.

1.8 **"Disclosure"** means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

1.9 **"Electronic Protected Health Information (ePHI)"** means Protected Health Information that is transmitted by electronic media or maintained as described in the definition of electronic media at 45 C.F.R. § 160.103.

1.10 **"Hardened Password"** after July 1, 2019 means a string of characters containing at least three of the following character classes: upper case letters; lower case letters; numerals; and special characters, such as an asterisk, ampersand or exclamation point.

1.10.1 Passwords for external authentication must be a minimum of 10 characters long.

1.10.2 Passwords for internal authentication must be a minimum of 8 characters long.

1.10.3 Passwords used for system service or service accounts must be a minimum of 20 characters long.

1.11 **"HIPAA"** means the Health Insurance Portability and Accountability Act of 1996, as amended, together with its implementing regulations, including the Privacy Rule, Breach Notification Rule, and Security Rule. The Privacy Rule is located at 45 C.F.R. Part 160 and Subparts A and E of 45 C.F.R. Part 164. The Breach Notification Rule is located in Subpart D of 45 C.F.R. Part 164. The Security Rule is located in 45 C.F.R. Part 160 and Subparts A and C of 45 C.F.R. Part 164.

1.12 **"HIPAA Rules"** means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Parts 160 and Part 164.

1.13 **"Medicare Data Use Requirements"** refers to the four documents attached and incorporated into this Exhibit as Schedules 1, 2, 3, and 4 that set out the terms and conditions Contractor must agree to for the access to and use of Medicare Data for the Individuals who are dually eligible in the Medicare and Medicaid programs.

1.14 **"Minimum Necessary"** means the least amount of PHI necessary to accomplish the purpose for which the PHI is needed.

1.15 **"Portable/Removable Media"** means any Data storage device that can be detached or removed from a computer and transported, including but not limited to: optical media (e.g. CDs, DVDs); USB drives; or flash media (e.g. CompactFlash, SD, MMC).

1.16 **"Portable/Removable Devices"** means any small computing device that can be transported, including but not limited to: handhelds/PDAs/Smartphones; Ultramobile PC's, flash memory devices (e.g. USB flash drives, personal media players); and laptops/notebook/tablet computers. If used to store Confidential Information, devices should be Federal Information Processing Standards (FIPS) Level 2 compliant.

1.17 **"PRISM"** means the DSHS secure, web-based clinical decision support tool that shows administrative data for each Medicaid Client and is organized to identify care coordination opportunities.

1.18 **"Protected Health Information"** or "PHI" has the same meaning as in HIPAA except that it in this Contract the term includes information only relating to individuals.

1.19 **"ProviderOne"** means the Medicaid Management Information System, which is the State's Medicaid payment system managed by HCA.

1.20 **"Security Incident"** means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

1.21 **"Tracking"** means a record keeping system that identifies when the sender begins delivery of Confidential Information to the authorized and intended recipient, and when the sender receives confirmation of delivery from the authorized and intended recipient of Confidential Information.

1.22 **"Transmitting"** means the transferring of data electronically, such as via email, SFTP, web-services, AWS Snowball, etc.

1.23 **"Transport"** means the movement of Confidential Information from one entity to another, or within an entity, that: places the Confidential Information outside of a Secured Area or system (such as a local area network); and is accomplished other than via a Trusted System.

1.24 **"Trusted System(s)"** means the following methods of physical delivery: (1) hand-delivery by a person authorized to have access to the Confidential Information with written acknowledgement of receipt; (2) United States Postal Service ("USPS") first class mail, or USPS delivery services that include Tracking, such as Certified Mail, Express Mail or Registered Mail; (3) commercial delivery services (e.g. FedEx, UPS, DHL) which offer tracking and receipt confirmation; and (4) the Washington State Campus mail system. For electronic transmission, the Washington State Governmental Network (SGN) is a Trusted System for communications within that Network.

1.25 **"U.S.C."** means the United States Code. All references in this Exhibit to U.S.C. chapters or sections will include any successor, amended, or replacement statute. The U.S.C. may be accessed at http://uscode.house.gov/

1.26 **"Unique User ID"** means a string of characters that identifies a specific user and which, in conjunction with a password, passphrase, or other mechanism, authenticates a user to an information system.

1.27 **"Use"** includes the sharing, employment, application, utilization, examination, or analysis, of Data.

2 Data Classification

2.1 The State classifies data into categories based on the sensitivity of the data pursuant to the Security policy and standards promulgated by the Office of the state of Washington Chief Information Officer. (See Section 4 of this Exhibit, Data Security, of Securing IT Assets Standards No. 141.10 in the State Technology Manual at https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets.)

The Data that is the subject of this Contract is classified as Category 4 – Confidential Information Requiring Special Handling. Category 4 Data is information that is specifically protected from disclosure and for which:

2.1.1 Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements;

2.1.2 Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

3 PRISM Access- N/A

4 Constraints on Use of Data

4.1 This Contract does not constitute a release of the Data for the Contractor's

discretionary use. Contractor must use the Data received or accessed under this Contract only to carry out the purpose of this Contract. Any ad hoc analyses or other use or reporting of the Data is not permitted without SBHASO's and HCA's prior written consent.

4.2 Data shared under this Contract includes data protected by 42 C.F.R. Part 2. In accordance with 42 C.F.R. § 2.32, this Data has been disclosed from records protected by federal confidentiality rules (42 C.F.R. Part 2). The federal rules prohibit Receiving Party from making any further disclosure of the Data that identifies a patient as having or having had a substance use disorder either directly, by reference to publicly available information, or through verification of such identification by another person unless further disclosure is expressly permitted by the written consent of the individual whose information is being disclosed or as otherwise permitted by 42 C.F.R. Party 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose (42 C.F.R. § 2.31). The federal rules restrict any use of the SUD Data to investigate or prosecute with regard to a crime any patient with a substance use disorder, except as provided at 42 C.F.R. § 2.12(c)(5) and § 2.65.

4.2.1 The information received under subsection 7.7 of the Contract is also protected by federal law, including 42 C.F.R. Part 2, Subpart D, § 2.53, which requires HCA and their Subcontractors to:

4.2.1.1 Maintain and destroy the patient identifying information in a manner consistent with the policies and procedures established under 42 C.F.R. § 2.16;

4.2.1.2 Retain records in compliance with applicable federal, state, and local record retention laws; and

4.2.1.3 Comply with the limitations on disclosure and Use in 42 C.F.R. Part 2, Subpart D, § 2.53(d).

4.3 Any disclosure of Data contrary to this Contract is unauthorized and is subject to penalties identified in law.

4.4 The Contractor must comply with the *Minimum Necessary Standard*, which means that Contractor will use the least amount of PHI necessary to accomplish the Purpose of this Contract.

4.4.1 Contractor must identify:

4.4.2 Those persons or classes of persons in its workforce who need access to PHI to carry out their duties; and

4.4.3 For each such person or class of persons, the category or categories of PHI to which access is needed and any conditions appropriate to such access.

4.4.4 Contractor must implement policies and procedures that limit the PHI disclosed to such persons or classes of persons to the amount reasonably necessary to achieve the purpose of the disclosure, in accordance with this Contract.

5 Security of Data

5.1 Data Protection

5.1.1 The Contractor must protect and maintain all Confidential Information gained by reason of this Contract, information that is defined as confidential under state or federal law or regulation, or Data that HCA has identified as confidential, against unauthorized use, access, disclosure, modification or loss. This duty requires the Contractor to employ reasonable security measures, which include restricting access to the Confidential Information by:

5.1.1.1 Allowing access only to staff that have an authorized business requirement to view the Confidential Information.

5.1.1.2 Physically securing any computers, documents, or other media containing the Confidential Information.

5.2 Data Security Standards

5.2.1 Contractor must comply with the Data Security Requirements set out in this section and the Washington OCIO Security Standard, 141.10, which will include any successor, amended, or replacement regulation (https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets.) The Security Standard 141.10 is hereby incorporated by reference into this Contract.

5.2.2 Data Transmitting

5.2.2.1 When transmitting Data electronically, including via email, the Data must be encrypted using NIST 800-series approved algorithms (http://csrc.nist.gov/publications/PubsSPs.html). This includes transmission over the public internet.

5.2.2.2 When transmitting Data via paper documents, the Contractor must use a Trusted System.

5.2.3 Protection of Data. The Contractor agrees to store and protect Data as described.

5.2.3.1 Data at Rest:

5.2.3.1.1 Data will be encrypted with NIST 800-series approved algorithms. Encryption keys will be stored and protected independently of the data. Access to the Data will be restricted to Authorized Users through the use of access control lists, a Unique User ID, and a Hardened Password, or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Systems that contain or provide access to Confidential Information must be located in an area that is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

5.2.3.2 Data stored on Portable/Removable Media or Devices

5.2.3.2.1 Confidential Information provided by SBHASO or HCA on Removable Media will be encrypted with NIST 800-series approved algorithms.
Encryption keys will be stored and protected independently of the Data.

5.2.3.2.2 HCA's Data must not be stored by the Contractor on Portable Devices or Media unless specifically authorized within the Contract. If so authorized, the Contractor must protect the Data by:

a. Encrypting with NIST 800-series approved algorithms. Encryption keys will be stored and protected independently of the data;

b. Controlling access to the devices with a Unique User ID and Hardened Password or stronger authentication method such as a physical token or biometrics;

c. Keeping devices in locked storage when not in use;

d. Using check-in/check-out procedures when devices are shared;

e. Maintaining an inventory of devices; and

f. Ensuring that when being transported outside of a Secured Area, all devices containing Data are under the physical control of an Authorized User.

5.2.3.3 Paper Documents. Any paper records containing Confidential Information must be protected by storing the records in a Secured Area that is accessible only to authorized personnel. When not in use, such records must be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

5.2.4 Data Segregation

5.2.4.1 HCA Data received under this Contract must be segregated or otherwise distinguishable from non-HCA Data. This is to ensure that when no longer needed by the Contractor, all of HCA's Data can be identified for return or destruction. It also aids in determining whether HCA's Data has or may have been compromised in the event of a security breach.

5.2.4.2 HCA's Data must be kept in one of the following ways:

5.2.4.2.1 On media (e.g. hard disk, optical disc, tape, etc.) which contains only HCA Data;

5.2.4.2.2 In a logical container on electronic media, such as a partition or folder dedicated to HCA's Data;

5.2.4.2.3 In a database that contains only HCA Data;

5.2.4.2.4 Within a database – HCA data must be distinguishable from non- HCA Data by the value of a specific field or fields within database records;

5.2.4.2.5 Physically segregated from non-HCA Data in a drawer, folder, or other container when stored as physical paper documents.

5.2.4.3 When it is not feasible or practical to segregate HCA's Data from non-HCA data, both HCA's Data

and the non-HCA data with which it is commingled must be protected as described in this Exhibit.

5.3 Data Disposition

5.3.1 Upon request by SBHASO or HCA, at the end of the Contract term, or when no longer needed, Confidential Information/Data must be returned to HCA or disposed of as set out below, except as required to be maintained for compliance or accounting purposes.

5.3.2 Media are to be destroyed using a method documented within NIST 800-88 (http://csrc.nist.gov/publications/PubsSPs.html).

5.3.3 For Data stored on network disks, deleting unneeded Data is sufficient as long as the disks remain in a Secured Area and otherwise meet the requirements listed in Section 4.b.iii, above. Destruction of the Data as outlined in this section of this Exhibit may be deferred until the disks are retired, replaced, or otherwise taken out of the Secured Area.

6 Data Confidentiality and Non-Disclosure

6.1 Data Confidentiality.

6.1.1 The Contractor will not use, publish, transfer, sell or otherwise disclose any Confidential Information gained by reason of this Contract for any purpose that is not directly connected with the purpose of this Contract, except:

6.1.1.1 as provided by law; or

6.1.1.2 with the prior written consent of the person or personal representative of the person who is the subject of the Confidential Information.

6.2 Non-Disclosure of Data

6.2.1 The Contractor will ensure that all employees or Subcontractors who will have access to the Data described in this Contract (including both employees who will use the Data and IT support staff) are instructed and aware of the use restrictions and protection requirements of this Attachment before gaining access to the Data identified herein. The Contractor will ensure that any new employee is made aware of the use restrictions and protection requirements of this Attachment before they gain access to the Data.

6.2.2 The Contractor will ensure that each employee or Subcontractor who will access the Data signs a non-disclosure of confidential information agreement regarding confidentiality and non-disclosure requirements of Data under this Contract. The Contractor must retain the signed copy of employee non-disclosure agreement in each employee's personnel file for a minimum of six years from the date the employee's access to the Data ends. The Contractor will make this documentation available to SBHASO or HCA upon request.

6.3 Penalties for Unauthorized Disclosure of Data

6.3.1 The Contractor must comply with all applicable federal and state laws and regulations concerning collection, use, and disclosure of Personal Information and PHI. Violation of these laws may result in criminal or civil penalties or fines.

6.3.2 The Contractor accepts full responsibility and liability for any noncompliance with applicable laws or this Contract by itself, its employees, and its Subcontractors.

7 Data Shared with Subcontractors

If Data access is to be provided to a Subcontractor under this Contract, the Contractor must include all of the Data security terms, conditions and requirements set forth in this Attachment in any such Subcontract.
However, no subcontract will terminate the Contractor's legal responsibility to HCA for any work performed under this Contract nor for oversight of any functions and/or responsibilities it delegates to any subcontractor. Contractor must provide an attestation by January 31, each year that all Subcontractor meet, or continue to meet, the terms, conditions, and requirements in this Attachment.

8 Data Breach Notification

8.1 The Breach or potential compromise of Data must be reported to the SBHASO Privacy Officer at **IClauson@co.kitsap.wa.us** and to the SBHASO Contract Manager at **Sjlewis@co.kitsap.wa.us** within five (5) business days of discovery. If the Contractor does not have full details, it will report what information it has, and provide full details within fifteen (15) business days of discovery. To the extent possible, these reports must include the following:

8.1.1 The identification of each non-Medicaid Individual whose PHI has been or may have been improperly accessed, acquired, used, or disclosed;

8.1.2 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;

8.1.3 A description of the types of PHI involved;

8.1.4 The investigative and remedial actions the Contractor or its Subcontractor took or will take to prevent and mitigate harmful effects, and protect against recurrence;

8.1.5 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 those Individuals should take to protect themselves; and

8.1.6 Any other information SBHASO or HCA reasonably requests.

8.2 The Contractor must take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or HCA including but not limited to 45 C.F.R. Part 164, Subpart D; RCW 42.56.590; RCW 19.255.010; or WAC 284-04-625.

8.3 The Contractor must notify SBHASO in writing, as described in 8.a above, within two (2) business days of determining notification must be sent to non-Medicaid Individuals.

8.4 At SBHASO's or HCA's request, the Contractor will provide draft Individual notification to HCA at least five (5) business days prior to notification, and allow HCA an opportunity to review and comment on the notifications.

8.5 At SBHASO's or HCA's request, the Contractor will coordinate its investigation and notifications with HCA and the Office of the state of Washington Chief Information Officer (OCIO), as applicable.

9 HIPAA Compliance

This section of the Attachment is the Business Associate Agreement (BAA) required by HIPAA. The Contractor is a "Business Associate" of SBHASO as defined in the HIPAA Rules.

9.1 HIPAA Point of Contact. The point of contact for the Contractor for all required HIPAA-related reporting and notification communications from this Section and all required Data Breach Notification from Section 8, is:

Salish Behavioral Health Administrative Services Organization
Attention: Ileea Clauson, Privacy Officer
614 Division St., MS-23
Port Orchard, WA 98366
Telephone: (360) 337-4833
Email: IClauson@co.kitsap.wa.us

9.2 Compliance. Contractor must perform all Contract duties, activities, and

tasks in compliance with HIPAA, the HIPAA Rules, and all attendant regulations as promulgated by the U.S. Department of Health and Human Services, Office for Civil Rights, as applicable.

9.3 Use and Disclosure of PHI. Contractor is limited to the following permitted and required uses or disclosures of PHI:

9.3.1 Duty to Protect PHI. Contractor must protect PHI from, and will use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164, Security Standards for the Protection of Electronic Protect Health Information, with respect to ePHI, to prevent unauthorized Use or disclosure of PHI for as long as the PHI is within Contractor's possession and control, even after the termination or expiration of this Contract.

9.3.2 Minimum Necessary Standard. Contractor will apply the HIPAA Minimum Necessary standard to any Use or disclosure of PHI necessary to achieve the purposes of this Contractor. See 45 C.F.R. § 164.514(d)(2) through (d)(5).

9.3.3 Disclosure as Part of the Provision of Services. Contractor will only Use or disclose PHI as necessary to perform the services specified in this Contract or as required by law, and will not Use or disclose such PHI in any manner that would violate Subpart E of 45 C.F.R. Part 164, Privacy of Individually Identifiable Health Information, if done by Covered Entity, except for the specific Uses and disclosures set forth below.

9.3.4 Use for Proper Management and Administration. Contractor may Use PHI for the proper management and administration of the Contractor or to carry out the legal responsibilities of the Contractor.

9.3.5 Disclosure for Proper Management and Administration. Contractor may disclosure PHI for the proper management and administration of Contractor, subject to HCA approval, or to carry out the legal responsibilities of the Contractor, provided the disclosures are required by law, or Contractor 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 the person notifies Contractor of any instances of which it is aware in which the confidentiality of the information has been Breached.

9.3.6 Impermissible Use or Disclosure of PHI. Contractor must report to the HIPAA Point of Contact, in writing, all Uses or disclosures of PHI not provided for by this Contract within five (5) business days of becoming aware of the unauthorized Use or disclosure of PHI, including Breaches of unsecured PHI as required at 45 C.F.R. §

164.410, Notification by a Business Associate, as well as any Security Incident of which Contractor becomes aware. Upon request by SBHASO or HCA, Contractor will mitigate, to the extent practicable, any harmful effect resulting from the impermissible Use or disclosure.

9.3.7 Failure to Cure. If SBHASO learns of a pattern or practice of the Contractor that constitutes a violation of Contractor's obligations under the term of this Attachment and reasonable steps by the Contractor do not end the violation, SBHASO may terminate this Contract, if feasible. In addition, if Contractor learns of a pattern or practice of its Subcontractor(s) that constitutes a violation of Contractor's obligations under the terms of their contract and reasonable steps by the Contractor do not end the violation, Contractor must terminate the Subcontract, if feasible.

9.3.8 Termination for Cause. Contractor authorizes immediate termination of this Contract by SBHASO, if SBHASO determines Contractor has violated a material term of this Business Associate Agreement. SBHASO may, at its sole option, offer Contractor an opportunity to cure a violation of this Business Associate Agreement before exercising a termination for cause.

9.3.9 Consent to Audit. Contractor must give reasonable access to PHI, its internal practices, records, books, documents, electronic data, and/or all other business information received from, or created, received by Contractor on behalf of SBHASO or HCA, to the Secretary of the United States Department of Health and Human Services (DHHS) and/or to HCA for use in determining compliance with HIPAA privacy requirements.

9.3.10 Obligations of Business Associate upon Expiration or Termination. Upon expiration or termination of this Contract for any reason, with respect to PHI received from SBHASO or HCA, or created, maintained, or received by Contractor, or any Subcontractors, on behalf of SBHASO or HCA, Contractor must:

9.3.10.1 Retain only that PHI which is necessary for Contractor to continue its proper management and administration or to carry out its legal responsibilities;

9.3.10.2 Return to SBHASO or HCA or destroy the remaining PHI that the Contractor or any Subcontractors still maintain in any form;

9.3.10.3 Continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164, Security Standards for Protection of Electronic Protected Health Information, with respect to ePHI to prevent Use or disclosure of the PHI,

other than as provided for in this Section, for as long as Contractor or any Subcontractor retains PHI;

9.3.10.4 Not Use or disclose the PHI retained by Contractor or any Subcontractors other than for the purposes for which such PHI was retained and subject to the same conditions section out in Section 9.3, Use and Disclosure of PHI, that applied prior to termination; and

9.3.10.5 Return to SBHASO or HCA or destroy the PHI retained by Contractor, or any Subcontractors, when it is no longer needed by Contractor for its proper management and administration or to carry out its legal responsibilities.

9.3.11 Survival. The obligations of Contractor under this Section will survive the termination or expiration of the Contract.

9.4 Individual Rights.

9.4.1 Accounting of Disclosures.

9.4.1.1 Contractor will document all disclosures, except those disclosures that are exempt under 45 C.F.R. § 164.528, of PHI and information related to such disclosures.

9.4.1.2 Within ten (10) business days of a request from SBHASO or HCA, Contractor will make available to HCA the information in Contractor's possession that is necessary for HCA to respond in a timely manner to a request for an accounting of disclosures of PHI by the Contractor. See 45 C.F.R. §§ 164.504(e)(2)(ii)(G) and 164.528(b)(1).

9.4.1.3 At the request of SBHASO or HCA, or in response to a request made directly to the Contractor by an Individual, Contractor will respond, in a timely manner and in accordance with HIPAA and the HIPAA Rules, to requests by Individuals for an accounting of disclosures of PHI.

9.4.1.4 Contractor record keeping procedures will be sufficient to respond to a request for an accounting under this section for the ten (10) years prior to the date on which the accounting was requested.

9.4.2 Access.

9.4.2.1 Contractor will make available PHI that it holds that is part of a Designated Record Set when requested by HCA or the Individual as necessary to satisfy HCA's

obligations under 45 C.F.R. § 164.524, Access of Individuals to Protected Health Information.

9.4.2.2 When the request is made by the Individual to the Contractor or if SBHASO or HCA ask the Contractor to respond to a request, the Contractor must comply with requirements in 45 C.F.R. § 164.524, Access of Individuals to Protected Health Information, on form, time and manner of access. When the request is made by HCA, the Contractor will provide the records to HCA within ten (10) business days.

9.4.3 Amendment.

9.4.3.1 If SBHASO or HCA amends, in whole or in part, a record or PHI contained in an Individual's Designated Record Set and SBHASO or HCA has previously provided the PHI or record that is the subject of the amendment to Contractor, then SBHASO will inform Contractor of the amendment pursuant to 45 C.F.R. § 164.526(c)(3), Amendment of Protected Health Information.

9.4.3.2 Contractor will make any amendments to PHI in a Designated Record Set as directed by SBHASO or HCA or as necessary to satisfy SBHASO's and HCA's obligations under 45 C.F.R. § 164.526, Amendment of Protected Health Information.

9.5 Subcontracts and other Third Party Agreements. In accordance with 45 C.F.R. §§ 164.502(e)(1)(ii), 164.504(e)(1)(i), and 164.308(b)(2), Contractor must ensure that any agents, Subcontractors, independent contractors, or other third parties that create, receive, maintain, or transmit PHI on Contractor's behalf, enter into a written contract that contains the same terms, restrictions, requirements, and conditions as the HIPAA compliance provisions in this Contract with respect to such PHI. The same provisions must also be included in any contracts by a Contractor's Subcontractor with its own business associates as required by 45 C.F.R. §§ 164.314(a)(2)(b) and 164.504(e)(5).

9.6 Obligations. To the extent the Contractor is to carry out one or more of HCA's obligation(s) under Subpart E of 45 C.F.R. Part 164, Privacy of Individually Identifiable Health Information, Contractor must comply with all requirements that would apply to HCA in the performance of such obligation(s).

9.7 Liability. Within ten (10) business days, Contractor must notify the HIPAA Point of Contact of any complaint, enforcement or compliance action initiated by the Office for Civil Rights based on an allegation of violation of the HIPAA Rules and must inform HCA of the outcome of that action. Contractor bears all responsibility for any penalties, fines or sanctions

imposed against the Contractor for violations of the HIPAA Rules and for any imposed against its Subcontractors or agents for which it is found liable.

9.8 Miscellaneous Provisions.

9.8.1 Regulatory References. A reference in this Contract to a section in the HIPAA Rules means the section as in effect or amended.

9.8.2 Interpretation. Any ambiguity in this Exhibit will be interpreted to permit compliance with the HIPAA Rules.

10 Inspection

SBHASO and HCA reserve the right to monitor, audit, or investigate the use of Personal Information and PHI of Individuals collected, used, or acquired by Contractor during the terms of this Contract. All SBHASO and HCA representatives conducting onsite audits of Contractor agree to keep confidential any patient-identifiable information which may be reviewed during the course of any site visit or audit.

11 Indemnification

The Contractor must indemnify and hold SBHASO and HCA and its employees harmless from any damages related to the Contractor's or Subcontractor's unauthorized use or release of Personal Information or PHI of Individuals.