PSC 21-630-8000-0017 A1
CFDA 93.778

STATE OF NEW MEXICO
HUMAN SERVICES DEPARTMENT
PROFESSIONAL SERVICES CONTRACT
AMENDMENT No. 1

THIS AMENDMENT No. 1 to Professional Services Contract (PSC) 21-630-8000-0017 is made and entered into by and between the State of New Mexico **Human Services Department**, hereinafter referred to as the "HSD," and the **Health Services Advisory Group, Inc.**, hereinafter referred to as the "Contractor".

The purpose of this Amendment is to add Sections 31 through 35 and Exhibit C, Business Associate's Agreement (BAA).

UNLESS OTHERWISE SET OUT BELOW, ALL OTHER PROVISIONS OF THE ABOVE REFERENCED AGREEMENT REMAIN IN FULL EFFECT AND IT IS MUTUALLY AGREED BETWEEN THE PARTIES THAT THE FOLOWING PROVIIONS OF THAT AGREEMENT ARE AMENDED AS FOLLOWS:

Section 31, Performance, is added to read as follows:

31. Performance.

In performance of this Agreement, the Contractor agrees to comply with and assume responsibility for compliance by its employees, its subcontractors, and/or Business Associates (BA), as applicable, with the following requirements:

A. All work will be performed under the supervision of the Contractor, the Contractor's responsible employees, and the Contractor's subcontracted staff.

B. Contractor agrees if Protected Health Information (PHI) as defined in 45 C.F.R. § 160.103, limited to PHI received from, or created on behalf of, HSD by Contractor; or Personally Identifiable Information (PII) as defined by the National Institute of Standards of Technology, limited to PII received from, or created on behalf of, HSD by Contractor pursuant to the Services; are collectively referred to as Confidential Information in Article 10 of this Agreement, made available to Contractor, shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and will not be divulged or made known in any manner to any person or entity except as may be necessary in the performance of this contract. Inspection by, or disclosure to, any person or entity other than an officer, employee, or subcontractor of the Contractor is prohibited.

C. Contractor agrees that it will account for all Confidential Information upon receipt and store such Confidential Information in a secure manner before, during, and after processing. In addition, all related output will be given the same level of protection by the Contractor as required for the source material.

D. The Contractor certifies that the Confidential Information processed during the performance of this Agreement will be purged from all electronic data storage components in

Contractor's facilities, including paper files, recordings, video, written records, printers, copiers, scanners and all magnetic and flash memory components of all systems and portable media, and no output will be retained by the Contractor at the time the work is completed or when this Contract is terminated. If immediate purging of all electronic data storage components is not possible, the Contractor certifies that any Confidential Information remaining in any storage component will be safeguarded to prevent unauthorized disclosures beyond the term of this Agreement as long as Contractor is in possession of such Confidential Information.

E. Any spoilage or any intermediate hard copy printout that may result during the processing of Confidential Information will be given to the HSD or his or her designee. When this is not possible, the Contractor will be responsible for the destruction (in a manner approved by the HSD) of the spoilage or any intermediate hard copy printouts, and will provide the HSD or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.

F. All of Contractor's computer systems, office equipment, written records, and portable media receiving, processing, storing, or transmitting Confidential Information must meet the requirements defined in relevant federal regulations such as HIPAA Privacy Rule (45 CFR Part 160 and Subparts A and E of Part 164), HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164), and/or any other Federal requirements that may apply to this contract. To meet functional and assurance requirements, the security features of the Contractor's environment must provide for security across relevant managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Confidential Information.

G. No work involving Confidential Information furnished under this Agreement will be subcontracted without prior written approval of the HSD.

H. The Contractor will maintain a list of its personnel, subcontractors, and/or business related entities with authorized access (electronic or physical) to HSD Confidential Information. Such list will be provided to the HSD and, upon request, to the federal agencies as required.

I. The Contractor will provide copies of signed acknowledgments for its staff and its subcontractors and/or Business Associates, to provide certification that relevant information security awareness and training was completed. These certifications will be provided to the HSD upon contract start and, at a minimum, annually thereafter during the term of this Agreement.

J. The HSD will have the right to terminate the contract if the Contractor or its subcontractors or Business Associates fail to provide the safeguards described above, consistent with the termination clause herein.

K. Upon request, the Contractor will provide the HSD copies of current policies and/or summaries of its current plans that document Contractor's privacy and security controls as they relate to HSD Confidential Information. This includes, at a minimum, any System Security Plans which describe the administrative, physical, technical, and system controls to be implemented for the security of the Department's Confidential Information. The plan shall include the requirement

for a Contractor notification to the Department Security Officer or Privacy Officer of breaches or potential breaches of information within three (3) days of their discovery.

L. All incidents affecting the compliance, operation, or security of the HSD's Confidential Information must be reported to the HSD. The Contractor shall notify the HSD of any instances of security or privacy breach issues or non-compliance promptly upon their discovery, but no later than a period of three (3) days (as stated above). Notification shall include a description of the privacy and security non-compliance issue and corrective action planned and/or taken.

M. The Contractor must provide the HSD with a summary of a corrective action plan (if any) to provide any necessary safeguards to protect PII from security breaches or non-compliance discoveries. The corrective action plan must contain a long term solution to possible future privacy and security threats to PII. In addition to the corrective action, the Contractor must provide updates as to the progress of all corrective measures taken until the issue is resolved. The Contractor shall be responsible for all costs of implementing the corrective action plan.

N. The HSD will have the right to seek remedies consistent with the liability terms of this contract Agreement and/or terminate the Agreement if the Contractor or its Subcontractors or Business Associates fail to provide the safeguards or to meet the security and privacy requirements to safeguard Confidential Information as described above, consistent with the liability and/or termination clauses herein.

O. All client files and patient records created or used to provide services under this Agreement, as between the parties, are at all times property of HSD. Upon termination of this Agreement for any reason, Business Associate shall return or destroy all PHI in its possession, and shall retain no copies of the PHI. In the event that Business Associate determines that returning or destroying the PHI is not feasible, Business Associate shall provide to the Department notification of the conditions that make return or destruction of PHI not feasible. Upon consideration and mutual agreement of the Parties that return or destruction of the PHI is infeasible, Business Associate shall agree, and require that its agents, affiliates, subsidiaries and subcontractors agree to the extension of all protections, limitations and restrictions required of Business Associate hereunder.

P. HSD Personally Identifiable Information (PII) cannot be accessed by HSD employees, agents, representatives, or contractors located offshore, outside of the United States territories, embassies, or military installations. Further, HSD PII may not be received, processed, stored, transmitted, or disposed of by information technology (IT) systems located offshore.

Section 32, Criminal/Civil Sanctions, is added to read as follows:

32. <u>Criminal/Civil Sanctions</u>.

A. It is incumbent upon Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C.552a. Specifically, 5 U.S.C.552a(i)(1), which is made applicable to contractors by 5 U.S.C.552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position,

has possession of or access to HSD records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully disclose the material in any manner to any person not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

B. Contractor agrees that granting access to PHI and PII must be preceded by certifying that each individual understands the HSD's applicable security policy and procedures for safeguarding PHI and PII. Contractors must maintain their authorization to access PHI and PII through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review.

Section 33, Inspection, is added to read as follows:

33. Inspection.

The HSD shall have the right, with 24 hour notice, to send its inspectors into the offices and plants of the Contractor to inspect the facilities and operations provided for the performance of any work related to PHI and PII under this Agreement. On the basis of such inspection specific measures may be required in cases where the Contractor is found to be noncompliant with contract safeguards.

Section 34, Contractor's Responsibility For Compliance With Laws and Regulations, is added to read as follows:

34. Contractor's Responsibility For Compliance With Laws and Regulations.

A. The Contractor is responsible for compliance with applicable laws, regulations, and administrative rules that govern the Contractor's performance of the Scope of Work of this Agreement and Exhibit A, including but not limited to, applicable State and Federal tax laws, State and Federal employment laws, State and Federal regulatory requirements and licensing provisions.

B. The Contractor is responsible for causing each of its employees, agents or subcontractors who provide services under this Agreement to be properly licensed, certified, and/or have proper permits to perform any activity related to the Scope of Work of this Agreement and Exhibit A.

C. If the Contractor's performance of its obligations under the terms of this agreement qualifies it as a Business Associate of the HSD as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and regulations promulgated thereunder, the Contractor agrees to execute the HSD Business Associate Agreement (BAA), attached hereto as Exhibit C, and incorporated herein by this reference, and comply with the terms of the BAA and subsequent updates.

Section 35, Contractor's Responsibility For Compliance With Laws and Regulations Relating To Information Technology, is added to read as follows:

35. Contractor's Responsibility For Compliance With Laws and Regulations Relating To Information Technology.

The Contractor agrees to monitor and control all its employees, subcontractors, consultants, or agents performing the Services under this PSC in order to assure compliance with the following regulations and standards insofar as they apply to Contractor's processing or storage of HSD's Confidential Information or other data:

1. The Federal Information Security Management Act of 2002 (FISMA);
2. The Health Insurance Portability and Accountability Act of 1996 (HIPAA);
3. The Health Information Technology for Technology for Economic and Clinical Health Act (HITECH Act);
4. Electronic Information Exchange Security Requirements, Guidelines, And Procedures For State and Local Agencies Exchanging Electronic Information With The Social Security Administration; and

NMAC 1.12.20, *et seq*. "INFORMATION SECURITY OPERATION MANAGEMENT".

Exhibit C, HIPPA Business Associate Agreement (BAA) is attached hereto and referenced in this amendment.

The remainder of this page intentionally left blank.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the date of the signature by the required approval authorities below.

By: DocuSigned by: kari Armijo 1BA9EB5EAD00499... Date: 6/4/2021
HSD Cabinet Secretary

Kari Armijo, Deputy Cabinet Secretary Signing electronically on behalf of D.S.

By: DocuSigned by: Mary Ellen Dalton 5A6EBD2BF28E43D... Date: 5/13/2021
Contractor

By: DocuSigned by: Sean Pearson 5318F28F172D40C... Date: 5/31/2021
HSD Chief Information Officer

Approved for legal sufficiency:

By: DocuSigned by: 32BE56E83D064CE... Date: 6/4/2021
HSD General Counsel

By: DocuSigned by: Danny Sandoval B66DFEE7DE10413... Date: 5/13/2021
HSD Chief Financial Officer

The records of the Taxation and Revenue Department reflect that the Contractor is registered with the Taxation and Revenue Department of the State of New Mexico to pay gross receipts and compensating taxes:

CRS ID Number: 02-350083-00-2

By: DocuSigned by: AnnMarie Lucero A1F73300ABB74BA... Date: 6/7/2021
Taxation & Revenue Department

This Agreement has been approved by the State Purchasing Contract Review Bureau

By: Date: June 25, 2021
Contract Review Bureau

Exhibit C

HIPAA Business Associate Agreement

This Business Associate Agreement ("BAA") is entered into between the New Mexico Human Services Department ("Department") and Health Services Advisory Group, Inc., hereinafter referred to as "Business Associate" , in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") as amended by Health Information Technology for Economic and Clinical Health Act of 2009 (the "HITECH Act"), including the Standards of the Privacy of Individually Identifiable Health Information and the Security Standards at 45 CFR Parts 160 and 164.

BUSINESS ASSOCIATE, by this PSC 21-630-8000-0017 A1 has agreed to provide services to, or on behalf of the HSD which may involve the disclosure by the Department to the Business Associate (referred to in PSC 21-630-8000-0017 A1 as "Contractor") of Protected Health Information. This Business Associate Agreement is intended to supplement the obligations of the Department and the Contractor as set forth in PSC 21-630-8000-0017 A1, and is hereby incorporated therein.

THE PARTIES acknowledge HIPAA, as amended by the HITECH Act, requires that Department and Business Associate enter into a written agreement that provides for the safeguarding and protection of all Protected Health Information which Department may disclose to the Business Associate, or which may be created or received by the Business Associate on behalf of the Department.

1. Definition of Terms

a. Breach. "Breach" has the meaning assigned to the term breach under 42 U.S.C. § 17921(1) [HITECH Act § 13400 (1)] and 45 CFR § 164.402.

b. Business Associate. "Business Associate", herein being the same entity as the Contractor in PSC 21-630-8000-0017 A1, shall have the same meaning as defined under the HIPAA standards as defined below, including without limitation Contractor acting in the capacity of a Business Associate as defined in 45 CFR § 160.103.

c. Department. "Department" shall mean in this agreement the State of New Mexico Human Services Department.

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

e. HIPAA Standards. "HIPAA Standards" shall mean the legal requirements as set forth in the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act of 2009, and the regulations and policy guidance, as each may be amended over time, including without limitation:

   i. Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information in 45 CFR Part 160 and Part 164, Subparts A and E.

ii. Breach Notification Rule. "Breach Notification" shall mean the Notification in the case of Breach of Unsecured Protected Health Information, 45 CFR Part 164, Subparts A and D

iii. Security Rule. "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Parts 160 and 164, Subparts A and C, including the following:

f. Security Standards. "Security Standards" hereinafter shall mean the Standards for the Protection of Electronic Protected Health Information at 45 CFR §164.306.

g. Administrative Safeguards. "Administrative Safeguards" shall mean the Standards for the Protection of Electronic Protected Health Information at 45 CFR §164.308.

h. Physical Safeguards. "Physical Safeguards" shall mean the Standards for the Protection of Electronic Protected Health Information at 45 CFR §164.310.

i. Technical Safeguards. "Technical Safeguards" shall mean the Standards for the Protection of Electronic Protected Health Information at 45 CFR §164.312.

j. Policies and Procedures and Documentation Requirements. "Policies and Procedures and Documentation Requirements" shall mean the Standards for the Protection of Electronic Protected Health Information at 45 CFR §164.316.

k. Protected Health Information. "Protected Health Information" or "PHI" shall have the same meaning as in 45 CFR §160.103, limited to the information created, maintained, transmitted or received by Business Associate, its agents or subcontractors from or on behalf of Department.

l. Required By Law. "Required By Law" shall have the same meaning as in 45 CFR §164.103.

m. Secretary. "Secretary" shall mean the Secretary of the U. S. Department of Health and Human Services, or his or her designee.

n. Covered Entity. "Covered Entity" shall have the meaning as the term "covered entity" defined at 45 CFR §160.103, and in reference to the party to this BAA, shall mean the State of New Mexico Human Services Department.

Terms used, but not otherwise defined, in this BAA shall have the same meaning as those terms in the HIPAA Standards. All terms used and all statutory and regulatory references shall be as currently in effect or as subsequently amended.

2. Obligations and Activities of Business Associate

a. General Rule of PHI Use and Disclosure. The Business Associate may use or disclose PHI it creates for, receives from or on behalf of, the Department to perform functions, activities or services for, or on behalf of, the Department in accordance with the specifications set forth in this BAA and in this PSC 21-630-8000-0017 A1; provided that such use or disclosure would not violate the HIPAA Standards if done by the Department; or as Required By Law.

i. Any disclosures made by the Business Associate of PHI must be made in accordance with HIPAA Standards and other applicable laws.

ii. Notwithstanding any other provision herein to the contrary, the Business Associate shall limit uses and disclosures of PHI to the "minimum necessary," as set forth in the HIPAA Standards.

iii. The Business Associate agrees to use or disclose only a "limited data set" of PHI as defined in the HIPAA Standards while conducting the authorized activities herein and as delineated in PSC 21-630-8000-0017 A1, except where a "limited data set" is not practicable in order to accomplish those activities.

iv. Except as otherwise limited by this BAA or PSC 21-630-8000-0017 A1, Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

v. Except as otherwise limited by this BAA or PSC 21-630-8000-0017 A1, Business Associate may disclose PHI for the proper management and administration of the Business Associate provided that the disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

vi. Business Associate may use PHI to report violations of law to appropriate federal and state authorities, consistent with 45 CFR § 164.502(j).

vii. Business Associate may use PHI to provide Data Aggregation services to the Department as permitted by the HIPAA Standards.

b. Safeguards. The Business Associate agrees to implement and use appropriate Security, Administrative, Physical and Technical Safeguards, and comply where applicable with subpart C of 45 C.F.R. Part 164, to prevent use or disclosure of PHI other than as required by law or as provided for by this BAA or PSC 21-630-8000-0017 A1, Business Associate shall identify in writing upon request from the Department all of those Safeguards that it uses to prevent impermissible uses or disclosures of PHI.

c. Restricted Uses and Disclosures. The Business Associate shall not use or further disclose PHI other than as permitted or required by this BAA or PSC 21-630-8000-0017 A1, the HIPAA Standards, or otherwise as permitted or required by law. The Business Associate shall not disclose PHI in a manner that would violate any restriction which has been communicated to the Business Associate.

i) The Business Associate shall not directly or indirectly receive remuneration in exchange for any of the PHI unless a valid authorization has been provided to the Business Associate that includes a specification of whether the PHI can be further exchanged for remuneration by the entity receiving the PHI of that individual, except as provided for under the exceptions listed in 45 C.F.R. §164.502 (a)(5)(ii)(B)(2).

ii) Unless approved by the Department, Business Associate shall not directly or indirectly perform marketing to individuals using PHI.

d. Agents. The Business Associate shall ensure that any agents that create, receive, maintain or transmit PHI on behalf of Business Associate, agree in writing to the same restrictions and conditions that apply to the Business Associate with respect to PHI, in accordance with

45 C.F.R. § 164.502(e)(1)(ii), and shall make that agreement available to the Department upon request. Upon the Business Associate's contracting with an agent for the sharing of PHI, the Business Associate shall provide the Department written notice of any such executed agreement.

e. Availability of Information to Individuals and the Department. Business Associate shall provide, at the Department's request, and in a reasonable time and manner, access to PHI in a Designated Record Set (including an electronic version if required) to the Department or, as directed by the Department, to an Individual in order to meet the requirements under 45 CFR § 164.524. Within three (3) business days, Business Associate shall forward to the Department for handling any request for access to PHI that Business Associate receives directly from an Individual. If requested by the Department, the Business Associate shall make such information available in electronic format as required by the HIPAA Standards to a requestor of such information and shall confirm to the Department in writing that the request has been fulfilled.

f. Amendment of PHI. In accordance with 45 CFR § 164.526, Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that the Department directs or agrees to, at the request of the Department or an Individual, to fulfill the Department's obligations to amend PHI pursuant to the HIPAA Standards. Within three (3) business days, Business Associate shall forward to the Department for handling any request for amendment to PHI that Business Associate receives directly from an Individual.

g. Internal Practices. Business Associate agrees to make internal practices, books and records, including policies, procedures and PHI, relating to the use and disclosure of PHI, available to the Department or to the Secretary within seven (7) days of receiving a request from the Department or receiving notice of a request from the Secretary, for purposes of the Secretary's determining the Department's compliance with the Privacy Rule.

h. PHI Disclosures Recordkeeping. Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for the Department to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with the HIPAA Standards and 45 CFR § 164.528. Business Associate shall provide such information to the Department or as directed by the Department to an Individual, to permit the Department to respond to an accounting request. Business Associate shall provide such information in the time and manner reasonably designated by the Department. Within three (3) business days, Business Associate shall forward to the Department for handling any accounting request that Business Associate directly receives from an individual.

i. PHI Disclosures Accounting. Business Associate agrees to provide to the Department or an Individual, within seven (7) days of receipt of a request, information collected in accordance with Section 2 (h) of this Agreement, to permit the Department to respond to a request for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528.

j. Security Rule Provisions. As required by 42 U.S.C. § 17931 (a) [HITECH Act Section 13401(a)] , the following sections as they are made applicable to business associates under the HIPAA Standards, shall also apply to the Business Associate: 1) Administrative Safeguards; 2) Physical Safeguards; 3) Technical Safeguards; 4) Policies and Procedures and Documentation Requirements; and 5) Security Standards. Additionally, the Business

Associate shall either implement or properly document the reasons for non-implementation of all safeguards in the above cited sections that are designated as "addressable" as such are made applicable to Business Associates pursuant to the HIPAA Standards.

k. Civil and Criminal Penalties. Business Associate agrees that it will comply with the HIPAA Standards as applicable to Business Associates, and acknowledges that it may be subject to civil and criminal penalties for its failure to do so.

l. Performance of Covered Entity's Obligations. To the extent the Business Associate is to carry out the Department 's obligations under the HIPAA Standards, Business Associate shall comply with the requirements of the HIPAA Standards that apply to the Department in the performance of such obligations.

m. Subcontractors. The Business Associate shall ensure that any subcontractors that create, receive, maintain or transmit PHI on behalf of Business Associate, agree in writing to the same restrictions and conditions that apply to the Business Associate with respect to PHI, with 45 C.F.R. § 164.502(e)(1)(ii), and shall make such information available to the Department upon request. Upon the Business Associate's contracting with an agent for the sharing of PHI, the Business Associate shall provide the Department written notice of any such executed agreement. Upon the Business Associate's contracting with a subcontractor for the sharing of PHI, the Business Associate shall provide the Department written notice of any such executed agreement.

3. Business Associate Obligations for Notification, Risk Assessment, and Mitigation

During the term of this BAA or PSC 21-630-8000-0017 A1, the Business Associate shall be required to perform the following pursuant to the Breach Notification Rule regarding Breach Notification, Risk Assessment and Mitigation:

Notification

a. Business Associate agrees to report to the Department Contract Manager or HIPAA Privacy and Security Officer any use or disclosure of PHI not provided for by this BAA or PSC 21-630-8000-0017 A1, and HIPAA Standards, including breaches of unsecured PHI as required by 45 C.F.R. § 164.410, as soon as it (or any employee or agent) becomes aware of the Breach, and in no case later than three (3) business days after it (or any employee or agent) becomes aware of the Breach, except when a government official determines that a notification would impede a criminal investigation or cause damage to national security.

b. Business Associate shall provide the Department with the names of the individuals whose unsecured PHI has been, or is reasonably believed to have been, the subject of the Breach and any other available information that is required to be given to the affected individuals, as set forth in 45 CFR §164.404(c), and, if requested by the Department, provide information necessary for the Department to investigate promptly the impermissible use or disclosure. Business Associate shall continue to provide to the Department information concerning the Breach as it becomes available to it, and shall also provide such assistance and further information as is reasonably requested by the Department.

Risk Assessment

c. When Business Associate determines whether an impermissible acquisition, use or disclosure of PHI by an employee or agent poses a low probability of the PHI being compromised, it shall document its assessment of risk in accordance with 45 C.F.R. §

164.402 (in definition of "Breach", ¶ 2) based on at least the following factors: (i) the nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; (ii) the unauthorized person who used the protected health information or to whom the disclosure was made; (iii) whether the protected health information was actually acquired or viewed; and (iv) the extent to which the risk to the protected health information has been mitigated. Such assessment shall include: 1) the name of the person(s) making the assessment, 2) a brief summary of the facts, and 3) a brief statement of the reasons documenting the determination of risk of the PHI being compromised. When requested by the Department, Business Associate shall make its risk assessments available to the Department.

d. If the Department determines that an impermissible acquisition, access, use or disclosure of PHI, for which one of Business Associate's employees or agents was responsible, constitutes a Breach, and if requested by the Department, Business Associate shall provide notice to the individuals whose PHI was the subject of the Breach. When requested to provide notice, Business Associate shall consult with the Department about the timeliness, content and method of notice, and shall receive the Department's approval concerning these elements. The cost of notice and related remedies shall be borne by Business Associate. The notice to affected individuals shall be provided as soon as reasonably possible and in no case later than 60 calendar days after Business Associate reported the Breach to the Department.

Mitigation

e. In addition to the above duties in this section, Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI, by Business Associate in violation of the requirements of this Agreement or the HIPAA Standards. Business Associate shall draft and carry out a plan of corrective action to address any incident of impermissible use or disclosure of PHI. If requested by the Department, Business Associate shall make its mitigation and corrective action plans available to the Department.

f. The notice to affected individuals shall be written in plain language and shall include, to the extent possible, 1) a brief description of the Breach, 2) a description of the types of Unsecured PHI that were involved in the Breach, 3) any steps individuals can take to protect themselves from potential harm resulting from the Breach, 4) a brief description of what the Business Associate and the Department are doing to investigate the Breach, to mitigate harm to individuals and to protect against further Breaches, and 5) contact procedures for individuals to ask questions or obtain additional information, as set forth in 45 CFR §164.404(c).

Notification to Clients

g. Business Associates shall notify individuals of Breaches as specified in 45 CFR §164.404(d) (methods of individual notice). In addition, when a Breach involves more than 500 residents of a State or jurisdiction, Business Associate shall, if requested by the Department, notify prominent media outlets serving such location(s), following the requirements set forth in 45 CFR §164.406.

4. Obligations of the Department to Inform Business Associate of Privacy Practices and Restrictions

a. The Department shall notify Business Associate of any limitation(s) in the Department's Notice of Privacy Practices, implemented in accordance with 45 CFR § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

b. The Department shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

c. The Department shall notify Business Associate of any restriction in the use or disclosure of PHI that the Department has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

d. The Department shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by the Department.

5. Term and Termination

a. Term. This BAA terminates concurrently with PSC 21-630-8000-0017 A1, except that obligations of Business Associate under this BAA related to final disposition of PHI in this Section 5 shall survive until resolved as set forth immediately below.

b. Disposition of PHI upon Termination. Upon termination of this PSC 21-630-8000-0017 A1 and BAA for any reason, Business Associate shall return or destroy all PHI in its possession, and shall retain no copies of the PHI. In the event that Business Associate determines that returning or destroying the PHI is not feasible, Business Associate shall provide to the Department notification of the conditions that make return or destruction of PHI not feasible. Upon mutual agreement of the Parties that return or destruction of the PHI is infeasible, Business Associate shall agree, and require that its agents, affiliates, subsidiaries and subcontractors agree, to the extension of all protections, limitations and restrictions required of Business Associate hereunder, for so long as the Business Associate maintains the PHI.

c. If Business Associate breaches any material term of this BAA, the Department may either:

i. provide an opportunity for Business Associate to cure the Breach and the Department may terminate this PSC 21-630-8000-0017 A1 and BAA without liability or penalty in accordance with Article 4, Termination, of PSC 21-630-8000-0017 A1, if Business Associate does not cure the breach within the time specified by the Department; or,

ii. immediately terminate this PSC 21-630-8000-0017 A1 without liability or penalty if the Department determines that cure is not reasonably possible; or,

iii. if neither termination nor cure are feasible, the Department shall report the breach to the Secretary.

The Department has the right to seek to cure any breach by Business Associate and this right, regardless of whether the Department cures such breach, does not lessen any right or remedy available to the Department at law, in equity, or under this BAA or PSC 21-630-8000-0017 A1, nor does it lessen Business Associate's responsibility for such breach or its

duty to cure such breach.

6. Penalties and Training.

Business Associate understands and acknowledges that violations of this BAA or PSC 21-630-8000-0017 A1 may result in notification by the Department to law enforcement officials and regulatory, accreditation, and licensure organizations. If requested by the Department, Business Associate shall participate in training regarding use, confidentiality, and security of PHI.

7. Miscellaneous

a. Interpretation. Any ambiguity in this BAA, or any inconsistency between the provisions of this BAA or PSC 21-630-8000-0017 A1, shall be resolved to permit the Department to comply with the HIPAA Standards.

b. Business Associate's Compliance with HIPAA. The Department makes no warranty or representation that compliance by Business Associate with this BAA or the HIPAA Standards will be adequate or satisfactory for Business Associate's own purposes or that any information in Business Associate's possession or control, or transmitted or received by Business Associate, is or will be secure from unauthorized use or disclosure. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.

c. Change in Law. In the event there are subsequent changes or clarifications of statutes, regulations or rules relating to this BAA or PSC 21-630-8000-0017 A1, the Department shall notify Business Associate of any actions it reasonably deems necessary to comply with such changes, and Business Associate shall promptly take such actions. In the event there is a change in federal or state laws, rules or regulations, or in the interpretation of any such laws, rules, regulations or general instructions, which may render any of the material terms of this BAA unlawful or unenforceable, or which materially affects any financial arrangement contained in this BAA, the parties shall attempt amendment of this BAA to accommodate such changes or interpretations. If the parties are unable to agree, or if amendment is not possible, the parties may terminate the BAA and PSC 21-630-8000-0017 A1 pursuant to its termination provisions.

d. 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 Department, Business Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

e. Assistance in Litigation or Administrative Proceedings. Business Associate shall make itself and any agents, affiliates, subsidiaries, subcontractors or workforce members assisting Business Associate in the fulfillment of its obligations under this BAA and PSC 21-630-8000-0017 A1 available to the Department, at no cost to the Department, to testify as witnesses or otherwise in the event that litigation or an administrative proceeding is commenced against the Department or its employees based upon claimed violation of the HIPAA standards or other laws relating to security and privacy, where such claimed

violation is alleged to arise from Business Associate's performance under this BAA or PSC 21-630-8000-0017 A1, except where Business Associate or its agents, affiliates, subsidiaries, subcontractors or employees are named adverse parties.

Additional Obligations. Department and Business Associate agree that to the extent not incorporated or referenced in any Business Associate Agreement between them, other requirements applicable to either or both that are required by the HIPAA Standards, those requirements are incorporated herein by reference.