COMMONWEALTH of VIRGINIA

Department of Medical Assistance Services

CHERYL ROBERTS
DIRECTOR

SUITE 1300
600 EAST BROAD ST
RICHMOND, VA 23219

BUSINESS ASSOCIATE AGREEMENT (BAA) to Contract/IAG # _____

PRIVACY AND SECURITY OF PROTECTED HEALTH INFORMATION

General Conditions

This BAA ("Agreement" or "BAA") is made as of the effective date of _____ , by the Department of Medical Assistance Services ("Covered Entity"), with offices at 600 East Broad Street, Richmond, Virginia, 23219, and_____("Business Associate"), with an office at _____. This is a non-exclusive agreement between the Covered Entity, which administers Medical Assistance, and the Business Associate named above.

The Covered Entity and Business Associate, as defined in 45 CFR 160.103, have entered into this Business Associate Agreement to comply with all applicable provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104-191, as amended, the current and future Privacy and Security requirements for such an Agreement, the Health Information Technology for Economic and Clinical Health (HITECH) Act, (P.L. 111-5) Section 13402, requirements for Business Associates regarding breach notification, as well as to protect the confidentiality and integrity of Protected Health Information (PHI) required by law, Department policy, professional ethics, and accreditation requirements.

DMAS and Business Associate ("parties") shall fully comply with all current and future provisions of the Privacy and Security Rules and regulations implementing HIPAA and HITECH, as well as Medicaid requirements regarding Safeguarding Information on Applicants and Recipients of 42 CFR 431, Subpart F, and Virginia Code § 32.1-325.3. The parties desire to facilitate the provision of or transfer of electronic PHI in agreed formats and to assure that such transactions comply with relevant laws and regulations. The parties intending to be legally bound agree as follows:

I. Definitions. As used in this Agreement, the terms below will have the following meanings:
   a. Business Associate has the meaning given such term as defined in 45 CFR 160.103.
   b. Covered Entity has the meaning given such term as defined in 45 CFR 160.103.
   c. Individual has the meaning given such term as defined in 45 CFR 160.103.
   c. Provider: Any entity eligible to be enrolled and receive reimbursement through Covered Entity for any Medicaid-covered services.

   d. The Medicaid Enterprise System (MES): a modular, flexible, and upgradable automated system that manages Medicaid claims processing and information retrieval, and meets standards set out by the Centers for Medicare and Medicaid Services (CMS). MES modules include, but are not limited to: Provider Services, Care Services, Pharmacy Services, Encounter Processing, Enterprise Data warehouse, Integrated Services and Appeals. The MES technical elements can be found at:
      i. https://www.medicaid.gov/medicaid/data-systems/certification/streamlined-modular-certification/index.html

e. Individually identifiable health information has the meaning given such term as defined in 45 CFR 160.103.
f. Protected Health Information (PHI) has the meaning given such term as defined in 45 CFR 160.103.
g. Breach has the meaning as that term is defined at 45 CFR 164.402.
h. Unsecured Protected Health Information has the meaning as that term is defined in45 CFR 164.402.
i. Transport Layer Security (TLS): A protocol (standard) that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

Terms used, but not otherwise defined, in this Agreement shall have the same meaning given those terms under HIPAA, the HITECH Act, and other applicable federal law.

II. Notices

1. Written notices regarding impermissible use, access, or disclosure of unsecured protected health information by the Business Associate shall be sent via email and general mail within 24 hours of the disclosure/suspected disclosure being discovered to the DMAS Privacy Officer (with a copy to the DMAS Contract Administrator in II.2) at:

DMAS Privacy Officer
Department of Medical Assistance Services
600 East Broad Street
Richmond, Virginia 23219
hipaaprivacy@dmas.virginia.gov

2. Other written notices to the Covered Entity should be sent via email or general mail to the attention of the designated DMAS Contract Administrator with copy to the Procurement and Contract Management Division (PCM) at:

Contact: Lorraine Bishop
Department of Medical Assistance Services
600 East Broad Street
Richmond, Virginia 23219

III. Special Provisions to General Conditions

1. Uses and Disclosure of PHI by Business Associate. The Business Associate
   a. May use, access, or disclose PHI received from the Covered Entity, if necessary, to carry out its legal responsibilities and for the proper management and administration of its business.
   b. Shall not use, access, or disclose PHI otherwise than as expressly permitted by this Agreement, or as required by law.
   c. Shall have a signed confidentiality agreement with all individuals of its workforce who have access to PHI. Copies of the signed confidentiality agreements shall be made available for inspection by DMAS upon request, and an attestation of the confidentiality agreement shall be submitted to DMAS annually or as changes are necessary.
   d. Shall not use, access, or disclose PHI to any member of its workforce except to those persons who have authorized access to the information and who have signed a confidentiality agreement.
   e. Shall ensure that any agents and subcontractors to whom it provides PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, agree in writing to all the same restrictions, terms, special provisions and general conditions in this BAA that apply to Business Associate. In addition, Business Associate shall ensure that any such subcontractor or agent agrees to implement reasonable and appropriate safeguards to protect Covered Entity's PHI. In instances in which one DMAS Business Associate is required to access DMAS PHI from another

DMAS Business Associate, the first DMAS Business Associate shall enter into a business associate agreement with the second DMAS Business Associate.

f. Shall provide Covered Entity access to its facilities used for the maintenance and processing of PHI, for inspection of its internal practices, books, records, and policies and procedures relating to the use, access, and disclosure of PHI, for purpose of determining Business Associate's compliance with this BAA.

g. Shall make its internal practices, books, records, and policies and procedures relating to the use, access, and disclosure of PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, available to the Secretary of Department of Health and Human Services (DHHS) or its designee and provide Covered Entity with copies of any information it has made available to DHHS under this section of this BAA.

h. Shall not directly or indirectly receive remuneration in exchange for the provision of any of Covered Entity's PHI, except with the Covered Entity's consent and in accordance with 45 CFR 164.502.

i. Shall make reasonable efforts in the performance of its duties on behalf of Covered Entity to use, access, disclose, and request only the minimum necessary PHI reasonably necessary to accomplish the intended purpose with the terms of this Agreement.

j. Shall comply with 45 CFR 164.520 regarding Notice of privacy practices for protected health information.

2. Safeguards - Business Associate shall

a. Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic PHI that it creates, receives, maintains or transmits on behalf of Covered Entity as required by the HIPAA Security Rule, 45 CFR Parts 160, 162, and 164 and the HITECH Act.

b. Include a description of such safeguards in the form of a Business Associate Data Security Plan.

c. In accordance with the HIPAA Privacy Rule, the Security Rule, and the guidelines issued by the National Institute for Standards and Technology (NIST), Business Associate shall use commercially reasonable efforts to secure Covered Entity's PHI through technology safeguards that render PHI unusable, unreadable and indecipherable to individuals unauthorized to access such PHI.

d. Business Associate shall not transmit PHI over the Internet or any other unsecure or open communication channel, unless such information is encrypted or otherwise safeguarded using procedures no less stringent than described in 45 CFR 164.312(e) below.

> (1) *Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.*
>
> 2) *Implementation specifications:*
>
> (i) *Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.*
>
> (ii) *Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.*

e. Business Associate shall provide a secure email transfer connection between Covered Entity's and Business Associate's email services to ensure encryption in transit for all messages. Business Associate will establish a bi-directional TLS encryption path between its own and Covered Entity's email servers (as required), which will be configured for current best security practices and standards.

The Business Associate shall provide acceptable means to encrypt individual email messages containing PHI that are sent to Covered Entity. Such means will not require any software to be installed on Covered Entity equipment

The Business Associate shall provide a solution, or work with Covered Entity to use a preexisting method, to securely receive and transfer files to Covered Entity's current and future file transfer for sharing capabilities.

3. Accounting of Disclosures - Business Associate shall
    a. Maintain an ongoing log of the details relating to any use, access, or disclosure of PHI outside the scope of this Agreement that it makes. The information logged shall include, but is not limited to;
        i. the date made,
        ii. the name of the person or organization receiving the PHI,
        iii. the recipient's (member) address, if known,
        iv. a description of the PHI used, accessed, or disclosed, and the reason for the use, access, or disclosure.
    b. Information logged by the Business Associate under part (a) shall be maintained by the Business Associate for at least six years from the date of the use, access, or disclosure.
    c. Provide this information to the Covered Entity to respond to a request by an individual for an accounting of use, access, or disclosure of PHI in accordance with 45 CFR 164.528.

4. Sanctions - Business Associate shall
    a. Implement and maintain disciplinary or adverse actions, which may include sanctions, for any employee, subcontractor, or agent who violates the requirements in this Agreement or the HIPAA privacy regulations.
    b. As requested by Covered Entity, take steps to mitigate any harmful effect of any such violation of this Agreement.

5. Business Associate also agrees to all of the following:
    a. In the event of any impermissible use, access, or disclosure of PHI or breach of unsecured PHI made in violation of this Agreement or any other applicable law, the Business Associate shall notify the DMAS Privacy Officer
        i. On the first day on which such impermissible use, access, or disclosure or breach is known or reasonably should be known by Business Associate or an employee, officer or agent of Business Associate other than the person committing the unauthorized or impermissible action, and

        ii. Written notification to DMAS Privacy Officer shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the Contractor to have been, accessed, acquired, used or disclosed during the impermissible use, access, or disclosure or breach. Business Associate shall confer with DMAS prior to providing any notifications to the public or to the Secretary of HHS.

    b. Breach Notification requirements.
        i. In addition to requirements in 5.a above, in the event of a breach or other impermissible use, access or disclosure by Business Associate of PHI or unsecured PHI, the Business Associate shall be required to notify in writing all affected individuals to include,
            a) a brief description of what happened, including the date of the impermissible use, access or disclosure or breach and the date the Business Associate discovered the impermissible use, access or disclosure or breach;
            b) a description of the types of unsecured PHI that were involved in the impermissible use, access or disclosure or breach;
            c) any steps the individuals should take to protect themselves from potential harm resulting from the impermissible use, access or disclosure or breach;
            d) a brief description of what Business Associate is doing to investigate the impermissible use, access or disclosure or breach, mitigate harm to individuals, and protect against any future impermissible use, access or disclosure or breach, and, if necessary,
            e) establishing and staffing a toll-free telephone line to respond to questions.

i. Prior to sending the notification to affected individuals, the Business Associate will submit the proposed notification to the DMAS Privacy Officer for review and approval. The Business Associate will include any revisions to the notification made by DMAS and only send the notification after it has been approved by the DMAS Privacy Officer.

ii. Business Associate shall be responsible for all costs associated with notification requirements in 5b, above.

iii. Written notices to all individuals and entities shall comply with 45 CFR 164.404(c)(2), 164.404(d)(1), 164.406, 164.408 and 164.412.

6. Amendment and Access to PHI - Business Associate shall

a. Make an individual's PHI available to Covered Entity within ten (10) days of an individual's request for such information as notified by Covered Entity.

b. Make PHI available for amendment and correction and shall incorporate any amendments or corrections to PHI within ten (10) days of notification by Covered Entity per 45 CFR 164.526.

c. Provide access to PHI contained in a designated record set to the Covered Entity, in the time and manner designated by the Covered Entity, or at the request of the Covered Entity, to an individual in order to meet the requirements of 45 CFR 164.524.

7. Termination

a. Covered Entity may immediately terminate this Agreement if Covered Entity determines that Business Associate has violated a material term of the Agreement.

b. This Agreement shall remain in effect unless terminated for cause by Covered Entity with immediate effect, or until terminated by either party with not less than thirty (30) days prior written notice to the other party, which notice shall specify the effective date of the termination; provided, however, that any termination shall not affect the respective obligations or rights of the parties arising under any Documents or otherwise under this Agreement before the effective date of termination.

c. Within the terms stated in the contract, Business Associate shall at the termination or expiration of this agreement return or destroy all PHI received from Covered Entity (or created or received by Business Associate on behalf of Covered Entity) that Business Associate still maintains in any form and retain no copies of such PHI.

d. Business Associate shall provide a written certification that all such PHI has been returned or destroyed, whichever is deemed appropriate by the Covered Entity. If such return or destruction is infeasible, Business Associate shall use such PHI only for purposes that make such return or destruction infeasible, and the provisions of this agreement shall survive with respect to such PHI.

e. Business Associate shall abide by 45 CFR 164.310(d) regarding the removal of PHI received by Business Associate.

8. Amendment

a. Upon the enactment of any law or regulation affecting the use, access, or disclosure of PHI, or the publication of any decision of a court of the United States or of this state relating to any such law, or the publication of any interpretive policy or opinion of any governmental agency charged with the enforcement of any such law or regulation, Covered Entity may, by written notice to the Business Associate, amend this Agreement in such manner as Covered Entity determines necessary to comply with such law or regulation.

b. If Business Associate disagrees with any such amendment, it shall notify Covered Entity in writing within thirty (30) days of Covered Entity's notice. If the parties are unable to agree on an amendment within thirty (30) days thereafter, either of them may terminate this Agreement by written notice to the other.

9. This Agreement shall have a document, attached hereto and made a part hereof, containing the following:

a. The names and contact information for at least one primary contact individual from each party to this Agreement.

b. A complete list of all individuals, whether employees or direct contractors of Business Associate, who shall be authorized to access Covered Entity's PHI
c. A list of the specific data elements required by Business Associate to carry out the purposes of this Agreement.
d. The purposes for which such data is required.
e. A description of how Business Associate intends to use, access, or disclose such data in order to carry out the purposes of this Agreement.

Business Associate agrees to update the above noted information as needed in order to keep the information current. Covered Entity may request to review the above-referenced information at any time, including for audit purposes, during the term of this Agreement.