



COMMONWEALTH of VIRGINIA
Department of Medical Assistance Services

PATRICK W. FINNERTY
DIRECTOR

SUITE 1300
600 EAST BROAD ST
RICHMOND, VA 23219
804/786-7933
804/225-4512 (FAX)
800/343-0634 (TDD)

**MASTER INTERAGENCY / BUSINESS ASSOCIATE AGREEMENT;
PRIVACY AND SECURITY OF PROTECTED HEALTH INFORMATION**

GENERAL CONDITIONS

THIS BUSINESS ASSOCIATE AGREEMENT is made as of **DATE** by the Department of Medical Assistance Services (herein referred to as "Covered Entity"), with an office at 600 East Broad Street, Suite 1300, Richmond, VA 23219 and «SchoolBoard» (here in referred to as "Business Associate"), a School District with an office at «Address1», «City_State_Zip».

This BUSINESS ASSOCIATE AGREEMENT (herein referred to as the "Agreement") constitutes a non-exclusive agreement between the Covered Entity, which administers Medical Assistance, and the Business Associate named above. The Business Associate is authorized to release specified information to participating Medicaid providers who choose to use the Business Associate as a means of obtaining eligibility information on Medicaid enrollees.

The Covered Entity and Business Associate, as defined in 45 CFR § 160.103 of the Final HIPAA Privacy Rule, have entered into this Business Associate Agreement to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Final Privacy regulation requirements for such an Agreement, as well as our duty to protect the confidentiality and integrity of Protected Health Information (PHI) required by law, Department policy, professional ethics, and accreditation requirements. Parties signing this Agreement shall fully comply with the provisions of the Regulations implementing HIPAA.

This Agreement will have, at a minimum, the following attachments: Chain of Trust Attachment, Data Security Plan Attachment, and Scope-of-Work Attachment.

The Department of Medical Assistance Services and «SchoolBoard» desire to facilitate the transfer of PHI in agreed formats and to assure that such transactions comply with relevant laws and regulations.

NOW THEREFORE, the parties, intending to be legally bound, agree as follows:

I. Definitions.

As used in this contract, the terms below will have the following meanings:

- a. Business Associate: A person or organization that performs a function or activity on behalf of the Covered Entity, but is not part of the Covered Entity's workforce. A business associate can also be a covered entity in its own right.
- b. Covered Entity: Includes 1) All health care providers who transmit any health information electronically in connection with standard financial or administrative transactions, 2) All health plans, 3) All health care clearinghouses. Covered entities are accountable for PHI. Centers for Medicaid and Medicare Services (CMS) (formerly HCFA), Medicare + Choice and Medicaid State plans are also covered entities.
- c. Provider: Any entity eligible to be enrolled and receive reimbursement through Covered Entity for any Medicaid-covered services.
- d. MMIS: The Medicaid Management Information System, the computer system that is used to maintain recipient, provider, and claims data for administration of the Medicaid program. This system is currently managed under a contract with First Health Services Corp., which serves as Covered Entity's fiscal agent.
- e. Protected Health Information (PHI): Individually identifiable information, including demographics, which relates to a person's health, health care, or payment for health care as specified in 45 CFR § 160.103 of the Final HIPAA Privacy Rule. HIPAA protects individually identifiable health information transmitted or maintained in any form.

II. Terms.

The terms of this Agreement are outlined in the Scope-of-Work Attachment. The Scope-of-Work will define and delineate DMAS and Business Associate's responsibilities under the conditions of this Agreement.

III. Notices.

Written notices to the Covered Entity should be sent through general mail to:

Contact: William J. Lessard, Jr., Director
 Provider Reimbursement Division
 Department of Medical Assistance Services
 600 East Broad Street, Suite 1300
 Richmond, Virginia 23219

IV. Special Provisions to General Conditions.

1. Use and Disclosure of PHI.

1.1 Use of PHI. Business Associate shall not use PHI otherwise than as expressly permitted by this Agreement, or as required by law. However, Business Associate may use PHI for purposes of managing its internal business processes relating to its functions under this Agreement. Business Associate shall be permitted to use and disclose PHI provided by Covered Entity as follows:

- (i) To the following persons: «Provider_Contact_Name», «Medicaid_Coordinator»; and
- (ii) For the following stated purposes: To access Medicaid and FAMIS Eligibility Data to be used for reimbursement to the Public School District and to assist Medicaid and FAMIS recipients in accessing Medicaid and FAMIS Services.

1.2 Disclosure to Third Parties. Business Associate 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 the same restrictions, terms, and conditions relating to PHI that apply to Business Associate in this Contract. Covered Entity shall have the option to review and approve all such written agreements between Business Associate and its agents and subcontractors prior to their effectiveness.

1.3 Disclosure and Confidentiality. Business Associate must have a confidentiality agreement in place with individuals of its workforce who have access to PHI. A sample Authorized Workforce Confidentiality Agreement is included as Exhibit B. Issuing and maintaining these confidentiality agreements will be the responsibility of the Business Associate. Covered Entity shall have the option to inspect the maintenance of said confidentiality agreements.

1.4 Disclosure to workforce. Business Associate shall not disclose PHI to any member of its workforce except to those persons who have authorized access to the information, who have received privacy training in PHI, and who have signed an agreement to hold the information in confidence.

2. Safeguards

2.1 Safeguards. Business Associate shall implement and maintain appropriate safeguards to prevent the use and disclosure of PHI, other than as provided in this Contract. A description of such safeguards in the form of a Business Associate Data Security Plan submitted by the Business Associate (see Exhibit A) shall be attached to this Contract and shall be considered a part hereof. Covered Entity's approval of such safeguards and any of Business Associate's measures to update or add safeguards during the Contract shall be required. Upon reasonable request, Business Associate shall give Covered Entity access for inspection and copying to Business Associate's facilities used for the maintenance or processing of PHI, and to its books, records, practices, policies and procedures concerning the use and disclosure of PHI, for the purpose of determining Business Associate's compliance with this Agreement.

3. Accounting of Disclosures.

3.1 Accounting of Disclosures. Business Associate shall maintain an ongoing log of the details relating to any disclosures of PHI it makes (including, but not limited to, the date made, the name of the person or organization receiving the PHI, the recipient's address, if known, a description of the PHI disclosed, and the reason for the disclosure). Business Associate shall, within thirty (30) days of Covered Entity's request, make such log available to Covered Entity, as needed for Covered Entity to provide a proper accounting of disclosures to its patients.

3.2 Disclosure to U.S. Department of Health and Human Services (DHHS). Business Associate shall make its internal practices, books, and records relating to the use 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 DHHS or its designee for purposes of determining Covered Entity's compliance with HIPAA and with the Privacy Regulations issued pursuant thereto. Business Associate shall provide Covered Entity with copies of any information it has made available to DHHS under this section of this Contract.

4. Reporting

4.1 Reporting Violations. Business Associate shall report to Covered Entity within thirty (30) days of discovery, any use or disclosure of PHI made in violation of this Contract or any law. Business Associate shall implement and maintain sanctions for any employee, subcontractor, or agent who violates the requirements in this Contract or the HIPAA privacy regulations. Business Associate shall, as requested by Covered Entity, take steps to mitigate any harmful effect of any such violation of this Contract.

5. Access and Amendment to PHI

5.1 Right of Access. Business Associate shall make an individual's PHI available to Covered Entity within thirty (30) days of an individual's request for such information as notified by Covered Entity. [Optional: PHI shall be provided as follows: floppy disk or CD ROM.

5.2 Right of Amendment. Business Associate shall make PHI available for amendment and correction and shall incorporate any amendments or corrections to PHI within thirty (30) days of notification by Covered Entity.

6. Termination

6.1 Termination. Covered Entity may immediately terminate this Contract if Covered Entity determines that Business Associate has violated a material term of this Contract. 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. Within thirty (30) days of expiration or earlier termination of this Contract, Business Associate shall 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. 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 Contract shall survive with respect to such PHI.

7. Amendment

7.1 Amendment. Upon the enactment of any law or regulation affecting the use 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. If Business Associate disagrees with any such amendment, it shall so 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.

EACH PARTY has caused this Agreement to be properly executed on its behalf as of the date first above written.

For: Virginia Department of Medical Assistance Services

For: «SchoolBoard»

By: Patrick W. Finnerty, Director

By: «Superintendent_Name», Superintendent,
«SchoolBoard»



COMMONWEALTH of VIRGINIA
Department of Medical Assistance Services

PATRICK W. FINNERTY
DIRECTOR

SUITE 1300
600 EAST BROAD ST
RICHMOND, VA 23219
804/786-7933
804/225-4512 (FAX)
800/343-0634 (TDD)

HIPAA BUSINESS ASSOCIATE CHAIN OF TRUST ATTACHMENT

THIS ATTACHMENT supplements and is made a part of the Business Associate Agreement (herein referred to as “Agreement”) by and between the Department of Medical Assistance Services (herein referred to as “Covered Entity”) and «SchoolBoard», «Address1», «City_State_Zip» (herein referred to as “Business Associate”).

BACKGROUND STATEMENTS

- A. Covered Entity and Business Associate are parties to an agreement pursuant to which Business Associate provides certain services to Covered Entity and, in connection with those services, Covered Entity discloses to Business Associate certain information (“Protected Health Information” as further defined below) that is subject to protection under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), Public Law 104-191; and
- B. Business Associate, as a recipient of Protected Health Information (PHI) from Covered Entity, is a “Business Associate” as that term is defined in HIPAA and regulations promulgated by the U.S. Department of Health and Human Services (DHHS) to implement certain provisions of HIPAA (herein “HIPAA Regulations”); and
- C. Pursuant to the HIPAA Regulations, all Business Associates of entities such as Covered Entity must, as a condition of doing business with Covered Entity, agree in writing to certain mandatory provisions regarding, among other things, the use and disclosure of PHI; and
- D. The purpose of this Attachment is to satisfy the requirements of the HIPAA Regulations, including, but not limited to, 45 CFR § 164.506, as the same may be amended from time to time.

IN CONSIDERATION OF THE FOREGOING, and of the desire of each party to continue providing or receiving services under the Agreement, the parties agree as follows:

1. Definitions.

Unless otherwise provided in this Attachment, capitalized terms have the same meaning as set forth in the HIPAA Regulations, 45 CFR 160-164. As used in this contract, the terms below will have the following meanings:

- a. Value-Added Network (VAN): A third party entity (e.g. vendor) that provides hardware and/or software communication services, which meet the security standards of telecommunication.

- b. Encryption: A security measure process involving the conversion of data into a format, which cannot be interpreted by outside parties.
2. **Scope-of-Use of PHI.** Business Associate may not:
- a. Use or otherwise disclose PHI (as defined in 45 CFR §160.103) it receives from Covered Entity for any purpose other than the purpose expressly stated in the Agreement;
 - b. Notwithstanding any other provisions of the Agreement, use or disclose PHI in the manner that violates or would violate the HIPAA regulations if such activity were engaged in by Covered Entity.
3. **Safeguards for the Protection of PHI.**
- a. Business Associate shall implement and maintain, and by this Agreement warrants that it has implemented, such safeguards as are necessary to ensure that the PHI disclosed by Covered Entity to Business Associate is not used or disclosed by Business Associate except as is provided in the Agreement.
 - b. As detailed in the Data Security Plan Attachment, the Business Associate Data Security Plan shall be attached hereto and incorporated herein by reference and outline the safeguards implemented and maintained by Business Associate to prevent unauthorized use or disclosure of PHI. Business Associate warrants and represents that the information in the Business Associate Data Security Plan is true, correct and accurate and that one or more persons knowledgeable about Business Associate's security systems and procedures has completed the Business Associate Data Security Plan on behalf of Business Associate. Business Associate acknowledges that Covered Entity is relying on the Business Associate Data Security Plan in selecting Business Associate as a Business Partner. Business Associate shall promptly notify Covered Entity of any material change to any aspect of its security safeguards. Notwithstanding any other provisions of this Agreement to the contrary, Covered Entity may terminate the Agreement without penalty if it determines, in its sole discretion, that any such changes or any diminution of Business Associate's reported security procedures render any or all of Business Associate's safeguards unsatisfactory to Covered Entity. Business Associate shall confirm in writing to Covered Entity, from time to time upon Covered Entity's request, the continued accuracy of the Business Associate Data Security Plan.
4. **Reporting of Unauthorized Use or Disclosure.** Business Associate shall promptly report to Covered Entity any use or disclosure of PHI of which Business Associate becomes aware that is not provided for or permitted in the Agreement. Business Associate shall permit Covered Entity to investigate any such report and to examine Business Associate's premises, records and practices.
5. **Use of Subcontractors.** To the extent that Business Associate uses one or more subcontractors or agents to provide services under the Agreement, and such subcontractors or agents receive or have access to the PHI, each such subcontractor or agent shall sign an agreement with Business Associate containing substantially the same provisions as this Attachment and further identifying Covered Entity as a third party beneficiary with rights of enforcement and indemnification from such subcontractors or agents in the event of any violations.
6. **Uses of Open Communication Channels; Encryption**
- a. Business Associate may not transmit PHI over the Internet or any other insecure or open communication channel unless such information is encrypted or otherwise safeguarded using procedures no less stringent than those described in 45 CFR § 164.312(e).
 - b. If Business Associate stores or maintains PHI in encrypted form, Business Associate shall,

promptly at Covered Entity's request, provide Covered Entity with the key or keys to unlock such information.

7. **Electronic Data Interchange (EDI)**

a. **Means of Transmission**

- i. Each party will transmit documents directly or through a third party value added network. Either party may select, or modify a selection of, a VAN upon thirty (30) days written notice.
- ii. Each party will be solely responsible for the costs of any VAN with which it contracts.
- iii. Each party will be liable to the other for the acts or omissions of its VAN while transmitting, receiving, storing or handling documents.
- iv. Each party is solely responsible for complying with the subscription terms and conditions of the VAN he or she selects, and for any and all financial liabilities resulting from that subscription agreement.

b. **Test Data Transmission**

Each party agrees to actively send and receive test data transmissions until routinely successful. Supplier agrees to receive redundant transmissions (e.g. faxed copy and electronic), if required by Covered Entity, for up to thirty (30) days after a successful EDI link is established.

c. **Garbled Transmissions**

If a party receives an unintelligible document, that party will promptly notify the sending party (if identifiable from the received document). If the sending party is identifiable from the document but the receiving party failed to give notice that the document is unintelligible, the records of the sending party will govern. If the sending party is not identifiable from the document, the records of the party receiving the unintelligible document will govern.

d. **Signatures**

Each authorized representative of a party will adopt a unique, verifiable electronic identification consisting of symbols or codes to be transmitted with each document. Use of the electronic identification will be deemed for all purposes to constitute a "signature" and will have the same effect as a signature on a written document. Each authorized representative of a party will maintain sole control of the use of his or her signature, and neither party will disclose the signatures of the other party to any unauthorized person.

e. **Enforceability and Admissibility**

- i. Any document properly transmitted pursuant to this Agreement will be deemed for all purposes (1) to be a "writing" or "in writing," and (2) to constitute an "original" when printed from electronic records established and maintained in the ordinary course of business.
- ii. Any document which is transmitted pursuant to the EDI terms of this Agreement will be as legally sufficient as a written, signed, paper document exchanged between the parties, notwithstanding any legal requirement that the document be in writing or signed. Documents introduced as evidence in any judicial, arbitration, mediation or administrative proceeding will be admissible to the same extent as business records maintained in written form.

8. **Authorized Alteration of PHI.**

- a. Business Associate acknowledges that the HIPAA regulations require Covered Entity to provide access to PHI to the subject of that information, if and when Business Associate makes any material alteration to such information. For purposes of this section, "Material Alteration" means any addition, deletion or change to the PHI of any subject other than the addition of indexing,

coding or other administrative identifiers for the purpose of facilitating the identification or processing of such information.

- b. Business Associate shall provide Covered Entity with notice of each material alteration to any PHI and shall cooperate promptly with Covered Entity in responding to any request made by any subject of such information to Covered Entity to inspect and/or copy such information.
- c. Business Associate may not deny Covered Entity access to any such information if, in Covered Entity's sole discretion, such information must be made available to the subject seeking access to it.
- d. Business Associate shall promptly incorporate all amendments or corrections to PHI when notified by Covered Entity that such information is inaccurate or incomplete.

9. **Audits, Inspection and Enforcement.**

- a. With reasonable notice, Covered Entity may inspect the facilities, systems, books and records of Business Associate to monitor compliance with this Attachment. Business Associate shall promptly remedy any violation of any term of this Attachment and shall certify the same to Covered Entity in writing. The fact the Covered Entity inspects, or fails to inspect, or has the right to inspect, Business Associate's facilities, systems and procedures does not relieve Business Associate of its responsibility to comply with this Attachment, nor does Covered Entity's failure to detect, or to detect but fail to call Business Associate's attention to or require Remediation of any unsatisfactory practice constitute acceptance of such practice or waiving of Covered Entity's enforcement rights.
- b. Business Associate further agrees to make its internal practices, books and records relating to the use and disclosure of PHI available to the Department of Health and Human Services (DHHS) or its agents for the purposes of enforcing the provisions of this Attachment and the HIPAA regulations.
- c. Covered Entity may terminate the Agreement without penalty if Business Associate repeatedly violates this Attachment or any provision hereof, irrespective of whether, or how promptly, Business Associate may remedy such violation after being notified of the same. In case of any such termination, Covered Entity shall not be liable for the payment of any services performed by Business Associate after the effective date of the termination, and Covered Entity shall be liable to Business Associate in accordance with the Agreement for services provided prior to the effective date of termination.
- d. Business Associate acknowledges and agrees that any individual who is the subject of PHI disclosed by Covered Entity to Business Associate is a third party beneficiary of this Attachment and may, to the extent otherwise permitted by law, enforce directly against Business Associate any rights such individual may have under this Attachment, the Agreement, or any other law, relating to or arising out of Business Associate's violation of any provision of this Attachment.

10. **Effect of Termination.** Upon the termination of the Agreement for any reason, Business Associate will return to Covered Entity or, at Covered Entity's direction, destroy, all PHI received from Covered Entity that Business Associate maintains in any form, recorded on any medium, or stored in any storage system within thirty (30) days of termination or expiration of this Agreement. A senior officer of Business Associate shall certify in writing to Covered Entity, within thirty (30) days after the termination or other expiration of the Agreement, that all PHI has been returned or disposed of as provided above and that Business Associate no longer retains any such PHI in any form. Business Associate shall remain bound by the provisions of this Attachment, even after termination of the Agreement, until such time as all PHI has been returned or otherwise destroyed as provided in this section.

11. **Indemnification.** Business Associate shall indemnify and hold Covered Entity harmless from and against all claims, liabilities, judgments, fines, assessments, penalties, awards, or other expenses, of any kind or

nature whatsoever, including, without limitation, attorney's fees, expert witness fees, and costs of investigation, litigation or dispute resolution, relating to or arising out of any breach or alleged breach of this Attachment by Business Associate.

12. **Disclaimer.** COVERED ENTITY MAKES NO WARRANTY OR REPRESENTATION THAT COMPLIANCE BY BUSINESS ASSOCIATE WITH THIS ATTACHMENT OR THE HIPAA REGULATIONS 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, NOR SHALL COVERED ENTITY BE LIABLE TO BUSINESS ASSOCIATE FOR ANY CLAIM, LOSS OR DAMAGE RELATED TO THE UNAUTHORIZED USE OR DISCLOSURE OF ANY INFORMATION RECEIVED BY BUSINESS ASSOCIATE FROM COVERED ENTITY OR FROM ANY OTHER SOURCE. BUSINESS ASSOCIATE IS SOLELY RESPONSIBLE FOR ALL DECISIONS MADE BY BUSINESS ASSOCIATE REGARDING THE SAFEGUARDING OF PHI.

13. **Certification.** Subject to compliance with Business Associate's security requirements, Covered Entity, or its authorized agents or contractors, may at Covered Entity's cost examine Business Associate's facilities, systems, procedures and records as may be required by such agents or contractors to certify to Covered Entity that Business Associate's security safeguards comply (or do not comply, as the case may be) with HIPAA, the HIPAA regulations, or this Attachment.

14. **Effect on Agreement.** Except as specifically required to implement the purposes of this Attachment, or to the extent inconsistent with this Attachment, all other terms of the Agreement shall remain in force and effect.

15. **Construction.** This Attachment shall be construed as broadly as necessary to implement and comply with HIPAA and the HIPAA Regulations. The parties agree that any ambiguity in this Attachment shall be resolved in favor of a meaning that complies and is consistent with HIPAA and the HIPAA Regulations.



COMMONWEALTH of VIRGINIA
Department of Medical Assistance Services

PATRICK W. FINNERTY
DIRECTOR

SUITE 1300
600 EAST BROAD ST
RICHMOND, VA 23219
804/786-7933
804/225-4512 (FAX)
800/343-0634 (TDD)

DATA SECURITY PLAN ATTACHMENT

THIS ATTACHMENT supplements and is made a part of the Business Associate Agreement (herein referred to as “Agreement”) by and between the Department of Medical Assistance Services (herein referred to as “Covered Entity”) and «SchoolBoard», «Address1», «City_State_Zip» (herein referred to as “Business Associate”).

I. General Requirements

The purpose of these requirements is to provide a framework for maintaining confidentiality and security of data compiled for the Business Associate or its subcontractors. This data is the property of the Covered Entity.

The Business Associate shall develop a written Business Associate Data Security Plan within thirty (30) days of the execution of this Agreement and make it available to the Covered Entity upon request. The Business Associate Data Security Plan shall describe the manner in which the Business Associate will use Covered Entity data and the procedures the Business Associate will employ to secure the data. The uses of Covered Entity data detailed in the Business Associate Data Security Plan shall not be in violation of purposes directly related to State Plan administration included in 42 CFR § 431.302¹. No other uses of Covered Entity data outside of the purposes stated in the Business Associate Data Security Plan will be allowed. The Business Associate agrees to restrict the release of information necessary to serve the stated purpose described in the Business Associate Data Security Plan. The Business Associate agrees that there will be no commercial use or marketing use of the Covered Entity’s data, which he or she receives or creates in fulfillment of his contractual obligations. Upon reasonable request, Business Associate shall give Covered Entity access for inspection and copying to Business Associate’s facilities used for the maintenance or processing of Protected Health Information (PHI), and to its books, records, practices, policies and procedures concerning the use and disclosure of PHI, for the purpose of determining Business Associate’s compliance with this Agreement.

The Business Associate agrees to fully comply with all federal and state laws and regulations, especially 42 CFR § 431, Subpart F, and Virginia Code Section 2.1-377, et. seq. Access to information concerning applicants or recipients must be restricted to individuals who are subject to standards of confidentiality comparable to those

¹ A. Federal requirements: Section 1902 (a) (7) of the Social Security Act (as amended) provides for safeguards which restrict the use or disclosure of information concerning Medicaid applicants and recipients to purposes directly connected with the administration of the State plan. Regulations at 42 CFR § 431.302 specify the purposes directly related to State plan administration. These include (a) establishing eligibility; (b) determining the amount of medical assistance; (c) providing services for recipients; and (d) conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to the administration of the plan.

Covered Entity imposes on its own workforce and vendors. The Business Associate attests that the data will be safeguarded according to the provisions of the written, Covered Entity approved, Business Associate Data Security Plan meeting the general requirements outlined in Part II of this document. The exact content of the Business Associate Data Security Plan will be negotiated between the Business Associate and Covered Entity's HIPAA Office of Privacy and Security since the general data processing environment of each Business Associate will be different. In no event shall the Business Associate provide, grant, allow, or otherwise give access to the data in contravention of the requirements of its approved Business Associate Data Security Plan. The Business Associate assumes all liabilities under both state and federal law in the event that data is disclosed in violation of 42 CFR § 431, Subpart F, or in violation of any other applicable state and federal laws and regulations.

The Business Associate shall dispose of all Covered Entity data upon termination of the contract according to provisions for such disposal contained in its Business Associate Data Security Plan. The Business Associate certifies that all data, whether electronic or printed, in any form: original, reproduced, or duplicated, has been disposed of in accordance with the provisions of the Business Associate Data Security Plan within thirty (30) days of completion of the project or termination of the contract. No copies, reproductions or otherwise, in whole or in part, in whatever form, of the data shall be retained by the Business Associate following completion of the contract. The Business Associate acknowledges that ownership of the data remains with the Covered Entity at all times.

II. Format for a Basic Business Associate Data Security Plan

1. State the nature of the requesting organization's relationship with Covered Entity. In the absence of a Business Associate Agreement or some other formal contractual relationship with Covered Entity, please provide an explanation of how the proposed use of Covered Entity data is directly related to State Plan Administration (see 42 CFR § 431.302).
2. Provide the name of the Business Associate's designated Information Security Officer, including full name, address, phone number and fax number. State the individual's relation to the business function.
3. Provide the names and position designations of all individuals who will have access to the data at or for the Business Associate.
4. State the exact purpose(s) for which the data will be used.
5. Describe the format (e.g., tape, paper, disk or electronic transfer) in which the Business Associate envisions receiving the required data from Covered Entity.
6. Describe the medium within the Business Associate's organization upon which the data will be stored (e.g., will the data be on a disk pack accessible by the Business Associate's mainframe; will the data reside on a floppy disk stored in a box of similar disks beside the Business Associate's PC; will the data be accessible to many users through a network on the Internet or on an Intranet?)
7. Describe the provisions the Business Associate is taking to physically safeguard Covered Entity data in whatever form it has been provided or created. As part of the Business Associate Data Security Plan for Covered Entity, the Business Associate must include a copy of any security plan, security policies, or security procedures currently in effect within the organization.
8. Identify all individuals (or entities) to whom the data will be distributed as a result of the business function.
9. Describe through what mechanisms and in what format the Business Associate proposes to make final work products available to Covered Entity.
10. Summarize, within the Business Associate Data Security Plan, the data retention and disposal requirements that exist in the Contract or Agreements with Covered Entity. If the Business Associate is subject to any other retention requirements, those requirements should be included in the Business Associate Data Security Plan.

11. Provide a statement of acknowledgement in the Business Associate Data Security Plan that all Covered Entity data, no matter how manipulated or summarized remains the property of Covered Entity.
12. Describe the provisions the Business Associate is taking to ensure continuity of service to Covered Entity in the event of an emergency or other catastrophic event causing Business Associate business interruption (where applicable).
13. Note the existence of any insurance or bonds carried by the Business Associate, which would protect the Business Associate and Covered Entity from contingent liability in the use of the data. Otherwise, provide a statement in the Business Associate Data Security Plan if no such insurance coverage exists.



COMMONWEALTH of VIRGINIA
Department of Medical Assistance Services

PATRICK W. FINNERTY
DIRECTOR

SUITE 1300
600 EAST BROAD ST
RICHMOND, VA 23219
804/786-7933
804/225-4512 (FAX)
800/343-0634 (TDD)

SCOPE-OF-WORK ATTACHMENT

THIS ATTACHMENT supplements and is made a part of the Business Associate Agreement (herein referred to as “Agreement”) by and between the Department of Medical Assistance Services (herein referred to as “Covered Entity”) and «SchoolBoard», «Address1», «City_State_Zip» (herein referred to as “Business Associate”).

III. General Terms

Covered Entity agrees to provide the following:

- a. [Covered Entity will provide technical assistance directly and through its MMIS fiscal agent to assist with use of any electronic formats, such as magnetic tape. Covered Entity will provide advance notice whenever possible before making changes to the format or to the codes used in the information processing.]
- b. [Covered Entity or its agent may conduct random audits of the Business Associate’s processes and require corrective action of deficiencies or, at Covered Entity’s option, may suspend or terminate access to the data by the Business Associate if the deficiencies are of such a severity to warrant such action. Immediate action is required to correct any deficiency that would compromise the privacy of individual enrollees’ information. Covered Entity will allow a reasonable time for the Business Associate to perform corrective action for other identified deficiencies.]

II. Business Associate agrees to the following:

- a. The Business Associate must adhere to all relevant confidentiality and privacy laws, regulations, and contractual provisions laid out in the Agreement. These laws and regulations include, but are not limited to: VA Code § 32.1-325.3, 12 VAC 30-20-90, § 1902(a)(7) of the Social Security Act, and 42 CFR § 431.300. The Business Associate shall have in place appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records.
- b. The Business Associate must have an agreement with each Medicaid provider who requests information from the Business Associate that binds the provider to the privacy and confidentiality laws and regulations referenced in paragraph (a) above and which prohibits use of the recipient information for any purpose other than administration of the Medicaid program. Each provider who requests information from the Business Associate must be identified by its Medicaid provider number to ensure entitlement to the data.
- c. If the Business Associate charges a fee for this service, the fee must be reasonable as determined by Covered Entity. Covered Entity will evaluate reasonableness by comparison with other vendors in this field or vendors providing similar services to the medical provider community or similar groups.

- d. The Business Associate must maintain a record of all inquiries for at least one year. This record must contain at least the following information: the provider name, recipient name, provider identification number, number of inquiries of each provider, the dates of the provider queries, and the dates the services were rendered. This record must be available for review by Covered Entity.
- e. The Business Associate shall be subject to random auditing by Covered Entity. Upon confirmation of any contract violation, a corrective action plan must be developed and implemented in a timely manner.
- f. The Business Associate shall reimburse Covered Entity or at Covered Entity's option, its agent, within thirty (30) days after identification of all reasonable costs and charges incurred by Covered Entity in providing all information previously specified and for the costs of random audits described in Section (e) above.
- g. The Business Associate shall indemnify and defend Covered Entity, its officers, and employees from and against any and all claims by any third party or parties, including Medicaid providers and Medicaid recipients, arising out of the Business Associate's execution or performance of this Agreement.
- h. Failure of the Business Associate to adhere to any part of the Agreement shall be sufficient reason for immediate suspension of access to the MMIS, with the right to terminate the Agreement as specified under Section IV, subsection 6 of the Business Associate Agreement.

III. Special Provisions

The Department of Medical Assistance Services agrees to provide Medicaid and FAMIS eligibility data to be used for reimbursement to the Public School District and to assist Medicaid and FAMIS recipients in accessing Medicaid and FAMIS services.



XYZ ORGANIZATION BUSINESS ASSOCIATE DATA SECURITY PLAN

14. State the nature of the requesting organization's relationship with DMAS. In the absence of a Business Associate Agreement or some other formal contractual relationship with DMAS, please provide an explanation of how the proposed use of DMAS data is directly related to State Plan Administration (see 42 CFR, Section 431.302).

XYZ is the contractor for DMAS contract # XXXX_XX for Preauthorization and Utilization Management Services.

15. Provide the name of the Business Associate's designated Information Security Officer, including full name, address, phone number and fax number. State the individual's relation to the business function.

Name
Title
Organization
Address
Phone
Fax

Ms. Doe oversees all IT operations at XYZ including connectivity to and data transfer between the DMAS Medicaid Management Information System (MMIS) and XYZ.

16. Provide the names and position designations of all individuals who will have access to the data at or for the Business Associate.

Associates' name, title, department

17. State the exact purpose(s) for which data will be used.

- 1) Medical Review
- 2) Report Generation

18. Describe the format (e.g., tape, paper, disk) in which the Business Associate envisions receiving the required data from DMAS.

Data is submitted from providers by telephone, fax, or mail for medical review purposes and is entered into the internal XYZ databases. Information for all review cases is stored on a XYZ Windows 2000 based server with Oracle 8i as the database management system. Data are backed up to magnetic tape at the end of each business day and stored offsite at X location.

19. Describe the medium within the Business Associate's organization upon which the data will be stored (e.g., will the data be on a disk pack accessible by the Business Associate's mainframe; will the data reside on a floppy disk stored in a box of similar disks beside the Business Associate's PC; will the data be accessible to many users through a network on the Internet or on an Intranet?)

To ensure confidentiality and security, XYZ maintains a filing process that includes staff assigned for file maintenance, file retrieval, file purging and file preparation for offsite storage. XYZ provides DMAS with access to all files during normal hours of operation.

XYZ maintains file storage facilities for on-site review of the previous six months of documentation. XYZ maintains offsite storage for files older than 6 months at X storage facility. Files stored at this facility are returned to our location within 24 hours of the retrieval request. Emergency same-day retrieval service is also available.

Information pertaining to all requests is entered at the Windows 2000 desktop using Visual Basic developed screens and is stored on our Windows 2000 based server with Oracle 8i as the database management system. Data is backed up to magnetic tape at the end of each business day and stored offsite at x location. Access to the server for administrative purposes is limited to the Systems Manager, John Doe, and the Database Administrator, Jane Doe. User access to the system and the case review data is controlled by Windows 2000 security provisions with additional access limitation imposed on the database side via Oracle. Both user ID's and passwords are required for access. Passwords are automatically aged by the system and must be changed by each user every thirty (30) days.

The Virginia Medicaid system is housed on a Hewlett Packard Pentium III 600 MHz server with 384k memory. Hard disk storage includes a RAID-5 disk array with four – 9.1 KB disk drives, a redundant power supply and tape backup. This system will have the same connectivity to DMAS MMIS as described above.

Data are never sent over the Internet. XYZ uses a secure 'internal' email system. Connectivity to our network is through a LAN in our Richmond office that then accesses our corporate email server via a dedicated frame delay connection line. We

do not use Internet email facilities to send any DMAS information. Please refer to the response to question 7 for further information.

XYZ currently connects to the MMIS at x location via a frame-relay connection from our Richmond office to DMAS.

Future Operating Environment

As required by our new contract with DMAS we will eventually connect to MMIS at X location directly, rather than connecting at DMAS. We will use a serial connection between the XYZ provided CSU/DSU and the X router. Based on the expected volume, we will provide a 64 KBPS frame relay dedicated data line to the current DMAS Fiscal Agent's data center. In the event that traffic increases significantly, additional bandwidth can be added. At both ends of the frame relay data line, XYZ will provide an ADTRAN TSU LT T1/Fractional T1 CSU/DSU. A public address subnet will be provided if requested by Fiscal Agent for router-to-router connection. There will be a serial router port connection to the CSU/DSU on the Fiscal Agent side of the connection. As required, only public IP addresses will be presented across the data line. No connections across the Internet will be used.

XYZ will employ terminal emulation software – Eicon Access for Windows 3270 – to access the system from our desktop personal computers. Our existing employees and the DMAS contract monitors currently use this software to provide 3270 emulation for access to the DMAS computer system.

While our existing computer system easily and effectively handles all the processing required to support the DMAS requirements, every automated system can be improved. To reduce our maintenance costs, improve system access to DMAS authorized users and improve reliability, we are enhancing our existing Visual Basic/Oracle 8i Based computer system to a configuration that can also employ a browser-based client under Windows 95/98/2000. This browser-based access will use a secure Virtual Private Network (VPN) connection to XYZ's Windows 2000 server supporting the Oracle 8i-database management system. This new environment will make it possible to extend access to the system to any DMAS approved user with access to the Internet, subject to encryption in the manner prescribed in the HCFA Internet Security Policy dated 11/24/1998.

Based on provider interest and approval of DMAS, we will develop ASP based forms to allow providers using their Internet connection to enter data about the pre-authorization request directly from their location – reducing or eliminating the need to fax this information to XYZ. Entry of information by the providers at the source of data to the XYZ maintained database means that errors and processing time associated with printing the fax, routing the fax to the appropriate reviewer and subsequent entry of the information to our computer system are eliminated.

20. Describe the provisions the Business Associate is taking to physically safeguard DMAS data in whatever form it has been provided or created. As part of the Business Associate Data Security Plan for DMAS, the Business Associate must include a copy of any security plan, security policies, or security procedures currently in effect within the organization.

Our data security and confidentiality plans are summarized and described below.

XYZ is well aware of the confidential nature of the information that we will receive and process, both in paper and electronic format. We also understand that all data provided by DMAS to XYZ remains the property of DMAS. We will use this data only for the activities needed to fully support all the requirements of this scope of work. In the event a need arises for use of the DMAS provided data for some other purpose, XYZ will obtain written permission from DMAS in advance of any use of this data. XYZ also agrees to follow federal and state confidentiality requirements as set forth in the then current Code of Federal Regulations and the then current Code of Virginia.

To ensure XYZ compliance with all of the confidentiality and security requirements associated with use and storage of health care information, all XYZ employees must adhere to the confidentiality rules and security procedures outlined in the XYZ Employee Notebook.

The notebook is updated as needed but at least every year to reflect current XYZ policies that its employees must adhere to. Every new employee is provided with a copy of the manual, and our Human Resources Department reviews the key section dealing with our confidentiality policy. This section includes information about:

- Access and disclosure of confidential information
- Responsibility for confidentiality vested in a single individual
- Research and statistical reporting
- Legal requests for information
- Disclosure, monitoring, review and evaluation
- Disclosure of privileged data and information to third parties
- Patient access to XYZ data and information
- Prospective employee background investigations
- Trustee and employee access and training
- Document accountability
- Building security
- Communications security, ADP security
- Subcontract requirements
- Responsibilities of medical review coordinators
- Requests for the generation of non-privileged information

➤ Penalties for disclosure of confidential information

HIPAA mandates new security standards to protect an individual's health information, while permitting the appropriate access and use of that information by health care providers, clearinghouses, and health plans. The standard mandates safeguards for physical storage and maintenance, transmission and access to individual health information regardless of the medium used. In addition to our institutionalization of confidentiality and security policies discussed above, XYZ will comply with all HIPAA data security requirements as needed.

These are some examples of steps we already have in place in:

- ◆ We have in place appropriate physical safeguards to protect data integrity, confidentiality and availability. Our offices are secure and require a key or swipe card for entry. Only XYZ employees and four DMAS contract monitors are granted these keys/cards. Visitors to XYZ facilities are required to register and wear visitor's passes. In addition a XYZ employee must escort them. Our computer servers and databases are housed in a locked room within our secure facility. Access to the computer room is limited to information technology personnel. XYZ employees escort maintenance personnel at all times. Smoke detectors and automated sprinkler systems are installed to protect from fire.
- ◆ We have developed and implemented administrative procedures to guard data integrity, confidentiality and availability. All employees are required to read and sign a non-disclosure agreement as a condition of employment. An employee handbook has been developed that details all employee responsibilities and acceptable conduct and the actions that may be taken in the event of improper conduct. Security awareness training is conducted periodically. All data is backed up on a daily basis and secured in a fireproof safe. Virus detection and correction software is installed on all PCs and corporate servers. Updates to this software are made on a bi-weekly basis.
- ◆ We have implemented technical security services to guard data integrity, confidentiality and availability. Access to our local area network and the services available on that network are limited to authorized users. The program manager for each program grants authorization and a unique user id and password are used to gain access. Passwords are automatically retired every thirty (30) days. Access to the automated applications and underlying databases requires a separate logon and password. Access is further controlled on a "need" basis, providing either no access, read only, or write access to data. Users are automatically denied access following 3 failed logon attempts. System logs record user logon attempts, and applications capture information about who has added, modified or deleted records.
- ◆ Finally we have implemented appropriate technical security mechanisms that include the processes to prevent unauthorized access to data that is transmitted over a communications network. Our Systems Administrator, who grants access to users only upon program manager approval, controls access to our network. Currently, remote access to our local area network (and thence to the applications and databases) is highly restricted, and is used only from system administration. As we migrate our applications to a "web" ready environment, we will only support dial-in access (to users approved by DMAS) via a limited number of dial up circuits or via the Internet using Virtual Private Network (VPN) technology. VPN supports user authentication via public-private key exchange and provides a secure connection from the remote user to our systems over an encrypted "virtual tunnel" through the Internet.

To ensure that our security policies and practices remain current, we will periodically assess our security risks and vulnerabilities and the mechanisms currently in place to mitigate those risks and vulnerabilities. Measures in addition to those described above will be added as needed.

21. Identify all individuals (or entities) to whom the data will be distributed as a result of the business function.

Data that identify individual recipients, providers or facilities will never be distributed to any entity outside DMAS except with the express prior consent of DMAS. Aggregated data may be used for provider training, legislative presentations etc., but also only with the prior consent of DMAS. Data may occasionally be requested by HCFA or to other federal oversight authorities for inclusion in multi-state studies, analyses or for other purposes, but again, will not be released without the consent of DMAS.

22. Describe through what mechanisms and in what format the Business Associate proposes to make final work products available to DMAS.

XYZ will use the mechanisms and formats preferred by DMAS to make final work products available. This may include electronic transmission, tape, diskette, hard copy, or any other medium requested by DMAS.

Currently the weekly, monthly, quarterly annual and ad hoc reports are sent to DMAS electronically and/or in hard copy format. XYZ does not electronically send any reports to DMAS that contain patient identifiable information.

23. Summarize, within the Business Associate Data Security Plan, the data retention and disposal requirements that exist in the Contract or Agreements with DMAS. If the Business Associate is subject to any other retention requirements, those requirements should be included in the Business Associate Data Security Plan.

To ensure confidentiality and security, XYZ maintains a filing process that includes staff assigned for file maintenance, file retrieval, file purging and file preparation for offsite storage. XYZ provides DMAS with access to all files during normal hours of operation.

XYZ currently maintains file storage facilities onsite and available for review for the previous 6 months of documentation. XYZ maintains offsite storage for files older than 6 months at x storage facility. Files stored at this facility are returned to our location within 24 hours of the retrieval request. Emergency same-day retrieval service is also available.

XYZ shreds all hard copy data that is not stored for retrieval. Any removable magnetic media that has been used for storage is degausses before disposal.

24. Provide a statement of acknowledgement in the Business Associate Data Security Plan that all DMAS data, no matter how manipulated or summarized remains the property of DMAS.

XYZ is well aware of the confidential nature of the information that we will receive and process, both in paper and electronic format. We also understand that all data provided by DMAS to XYZ remains the property of DMAS. We will use this data only for the activities needed to fully support all the requirements of this scope of work. In the event a need arises for use of the DMAS provided data for some other purpose, XYZ will obtain written permission from DMAS in advance of any use of this data. XYZ also agrees to follow federal and state confidentiality requirements as set forth in the then current Code of Federal Regulations and the then current Code of Virginia.

25. Describe the provisions the Business Associate is taking to ensure continuity of service to DMAS in the event of an emergency or other catastrophic event causing Business Associate business interruption (where applicable).

XYZ has instituted a policy detailing our procedures for preauthorization during loss of connectivity. The following policies may be found in our XYZ -- Virginia Operations Policy and Procedures Manual and are also attached to this document.

- ◆ Utilization Review (Inpatient) Procedure for Loss of Connectivity.
- ◆ Utilization Management (Inpatient) Procedure for Loss of XYZ Database
- ◆ Prior-Authorization (Outpatient) Procedure for Loss of Connectivity
- ◆ Prior-Authorization (Outpatient) Procedure for Loss of XYZ Database
- ◆ Behavioral Health Review Procedure for Loss of Connectivity
- ◆ Behavioral Health Review Procedure for Loss of XYZ Database
- ◆ Community Based Care Review Procedure for Loss of Connectivity
- ◆ Community Based Care Review Procedure for Loss or XYZ Database

26. Note the existence of any insurance or bonds carried by the Business Associate, which would protect the Business Associate and DMAS from contingent liability in the use of the data. Otherwise, provide a statement in the Business Associate Data Security Plan if no such insurance coverage exists.

Our current Managed Care E&O Policy does cover "Medical Information Protection for claims arising out of the inadvertent release of medical information/records." Our underwriter is:

Name
Title
Organization
Address
License #
Phone
Fax

Attachments:

Enclosed are additional documents including Policies and Procedures that XYZ has issued in order to meet the guidelines of the Data Security Plan.



COMMONWEALTH of VIRGINIA
Department of Medical Assistance Services

PATRICK W. FINNERTY
DIRECTOR

SUITE 1300
600 EAST BROAD ST
RICHMOND, VA 23219
804/786-7933
804/225-4512 (FAX)
800/343-0634 (TDD)

Authorized Workforce Confidentiality Agreement

This Agreement between «SchoolBoard», «Address1», «City_State_Zip» [Business Associate Name] and _____ (please print), an employee of _____ hereby acknowledges that [the Entity's] records and documents are subject to strict confidentiality requirements imposed by state and federal law including 42 CFR § 431 Subpart F, Virginia Code Section 2.1-377, 12 VAC 30-20-90, et. seq.

I (initial) _____ acknowledge that my supervisor, or whoever administers the data, has reviewed with me the appropriate provisions of both state and federal laws including the penalties for breaches of confidentiality.

I (initial) _____ acknowledge that my supervisor, or whoever administers the data, has reviewed with me the confidentiality and security policies of [the entity].

I (initial) _____ acknowledge that my supervisor or, whoever administers the data, has reviewed with me the confidentiality and security policies of our organization.

I (initial) _____ acknowledge that unauthorized use, dissemination or distribution of Virginia Department of Medical Assistance Services (DMAS) confidential information is a crime.

I (initial) _____ hereby agree that I will not use, disseminate or otherwise distribute confidential records or said documents or information either on paper or by electronic means other than in performance of the specific job roles I am authorized to perform.

I (initial) _____ also agree that unauthorized use, dissemination or distribution of confidential information is grounds for immediate termination of my employment or contract with [the entity] and may subject me to penalties both civil and criminal.

Signed