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 [name Business Associate] (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 § 431.302[1]. 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

[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.

recipients must be restricted to individuals who are subject to standards of confidentiality comparable to those 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.