PINNACLE HEALTH

MEMORANDUM

TO: Vendors/Independent Contractors/Consultants

FROM: Raymond R. Hebert
Compliance and Privacy Officer

SUBJECT: Business Associate Agreements and the Healthcare Insurance Portability and Accountability Act (HIPAA) of 1996

The Health Insurance Portability and Accountability Act of 1996 or HIPAA is the most sweeping legislation to affect the health care industry in over 30 years. HIPAA regulations contain three major objectives:

1. Portability of health insurance.

2. Extension of fraud and abuse prevention measures.

3. Administrative simplification which includes:

   a. Standardization of electronic data interchange.

   b. Privacy and security protection for individually identifiable health information (PHI).

The HIPAA regulations for the Standards for Privacy of Individually Identified Health Information (45 CFR Parts 160 and 164) take effect in April 2003. Individually Identified Health Information (IIHI) that is covered under the act is called Protected Health Information or PHI. Vendors, Independent Contractors, Consultants, etc. that have access to PHI and are not part of Pinnacle's workforce may be considered Business Associates for HIPAA purposes. If you are a Business Associate we are required to have a Business Associate Agreement signed by you (if you are an independent contractor/sole proprietor) or your employer.

A Business Associate performs one or more of the following functions:

1. Receives PHI from the covered entity and uses PHI on behalf of the covered entity.

2. Creates PHI on behalf of the covered entity.

3. Provides services to the covered entity and has access and uses PHI.

To familiarize you with HIPAA terminology that relates to Business Associates the following definitions are provided:

Business Associate: HIPAA permits a covered entity (Pinnacle Health) to disclose PHI to a Business Associate. The Business Associate performs a function on behalf of a covered entity using individually identifiable information. A Business Associate or third party may create and receive PHI only if the covered entity obtains satisfactory assurances that the Business Associate will appropriately safeguard the information. These safeguards are listed in a Business Associate Agreement.

Business Associate Agreement: Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) final privacy rule, agreements between a health care organization and a Business Associate must provide that the Business Associate shall:

- Only use or disclose protected health information (PHI) as permitted (1) under the agreement and (2) by covered entities under the final rule.
- Use "appropriate safeguards" to prevent use or disclosure of PHI except as permitted by the agreement.
- Report any known misuse of PHI to the covered entity.

A Business Associate must agree to:

- Impose the same requirements on its subcontractors and agents.
- Make PHI available as required by the final rule.
- Provide an accounting of disclosure as required by the final rule.
- Make its internal practices, books, and records relating to use and disclosure of PHI available to the U.S. Department of Health and Human Services (for purposes of an investigation).

Agreements with Business Associates must also provide that:

- The covered entity may terminate the agreement if the covered entity determines that the Business Associate has breached a material term of the agreement.
- Upon termination of the relationship, the Business Associate will return or destroy all PHI, if feasible (or extend the protections).

Covered Entity: An entity that is required to comply with the requirements of HIPAA administrative simplification regulations. Covered entities are health plans, health care clearinghouses, and health care providers that transmit any health information in electronic form in connection with a standard transaction. Pinnacle Health is a covered entity under HIPAA.

Protected Health Information (PHI): The HIPAA regulations define "individually identifiable health information" as information collected from an individual that is created or received from a health care provider and relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual which identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. This includes demographic information. Examples of PHI include:

- Name and any of the following:
- Geographic subdivision smaller than a state
- Names of relatives and/or employer
- All elements of dates
- Telephone and/or Fax numbers
- E-mail address and IP addresses
- Social Security Number
- Medical record number
- Health plan beneficiary number
- Account number
- License number
- Other device serial numbers
- Web URL
- IP Address
- Finger or voice prints
- Photos
- Any identifying number or code

To determine if you are a Business Associate, please complete the Business Associate Determination Checklist for HIPAA.

If you have any questions, please feel free to contact me at (717)231-8211, fax (717)231-8157, or e-mail rhebert@pinnaclehealth.org.

Revised: February 2003

jeh