DHHS POLICIES AND PROCEDURES

Section VIII:	**Privacy and Security**
Title:	**Privacy Manual**
Chapter:	**Administrative Policies, Business Associates (Internal/External)**
Current Effective Date:	**10/23/19**
Revision History:	**10/23/19; 8/21/13; 5/1/05**
Original Effective Date:	**4/14/03**

Purpose

To ensure that all individuals or organizations that perform specific functions, activities, or services for the North Carolina Department of Health and Human Services (NC DHHS) agencies involving the sharing of individually identifiable health information are appropriately identified according to The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule as a "**business associate"**; and to further ensure that **"agreements"** are developed to support such contractual relationships, as appropriate. ***This policy shall apply to the following DHHS agencies:***

- ***HIPAA covered health care components and***
- ***Internal business associates***.

Background

DHHS workgroups that must comply with the HIPAA Privacy Rule are referred to as "covered health care components". The HIPAA Privacy Rule requires covered health care components to identify persons or entities that provide specific functions, activities, or services that involve the use, creation, or disclosure of individually identifiable health information for, or on their behalf. Such entities are referred to as business associates.

It should be noted that the Omnibus Final Rule has expanded the definition of a business associate to include:

- Any downstream subcontractor that creates, maintains, receives or transmits protected health information (PHI) on behalf of a business associate, even if they have an indirect relationship with the covered entity;
- Health information organizations, e-prescribing gateways, or other persons that provide data transmission services to a covered entity that require routine access to PHI; and
- Any person that offers a personal health record to individuals on behalf of a covered entity.

Because the department had been determined to be a hybrid entity, each DHHS division and office was required to identify components that are covered by this HIPAA requirement. Although some components were determined not to be covered health care components under HIPAA, they do perform functions, activities, or services that involve the sharing of individually identifiable health information for, or on behalf of, covered health care components thus creating business associate

relationships within this department. Such persons or entities ***within*** DHHS are health care components that are referred to as **"internal business associates"**.

Components in other NC state government departments/agencies or external contractors ***outside*** of DHHS that perform functions, activities, or services for, or on behalf of, a DHHS covered health care component, and involve the use, creation, or disclosure of individually identifiable health information are referred to as **"external business associates"**.

Functions, activities, and services performed by business associates that involve the use, creation, or disclosure of individually identifiable health information may include claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and re-pricing.

Policy

Business Associates

DHHS covered health care components are required to identify their ***internal*** business associates by recognizing all of the other divisions/offices (or portions thereof) within the department that perform specific functions, activities, or services for, or on behalf of, the covered component when such functions or activities involve the sharing of individually identifiable health information.

DHHS ***internal*** business associates must also identify their internal business associates by recognizing any other health care component(s) within DHHS that perform such functions, activities, or services for, or on behalf of, the internal business associate that involves the sharing of individually identifiable health information.

DHHS covered health care components and internal business associates must identify their ***external*** business associates by recognizing other NC state government departments/agencies and external contractors (public and private) that perform specific functions, activities, or services for, or on behalf of, the covered component or the internal business associate when such functions, activities, or services involve the sharing of individually identifiable health information.

Business associates, as well as their subcontractors who have access to PHI, are now directly liable for failure to comply with the HIPAA Privacy and Security Rules. If they fail to do so, they can be assessed civil and criminal penalties.

Incidental access to individually identifiable health information while performing duties that do not typically involve the use or disclosure of such information generally does not constitute a business associate relationship.

Business Associate Agreements

DHHS covered health care components and internal business associates must initiate agreements with their external business associates in order to share individually identifiable health information while

performing specific functions, activities, or services for, or on behalf of, the covered health care component or the internal business associate.

It is the responsibility of covered health care components and internal business associates to execute agreements with external business associates that provide satisfactory assurance that the business associate will appropriately safeguard individually identifiable health information.

A Business Associate is responsible for entering into Business Associate Agreements with its subcontractors. In turn, a subcontractor is responsible for entering into Business Associate Agreements with any of its own subcontractors "down the chain" of information flow.

Business Associate Agreements must be revised using the new DHHS standard BAA form, per the timeline stipulated by the OCR.

This revised Business Associate Agreement template, developed by the NC Office of the Attorney General, is required when contracts are initiated by DHHS staff. Such addenda must be attached to the department's standard contracting template as specified in the DHHS Purchasing and Contracts Manual.

Certain external contractors may be considered part of the HIPAA covered component's ***workforce***, and therefore will not require a business associate agreement if the following criteria apply:

- The workstation of the person under contract is on the covered health care component's premises and
- The person performs a substantial proportion of his/her activities at this location.

Any external contractor who is considered part of the covered health care component's workforce must comply with that component's privacy policies and procedures.

BAA are not required with contract agreements between agencies within DHHS since the DHHS Privacy Policy Manual applies to all DHHS agencies.

Disclosure of individually identifiable health information from one health care provider to another for treatment, consultation, or referral does not require a business associate agreement. (Note: For MH/DD/SAS agencies, a business associate agreement would not be required, but those agencies would have to initiate either a "service provider agreement", according to NC General Statutes, or would have to secure client authorization to disclose health information to a health care provider outside the agency.)

A business associate agreement is also not required when individually identifiable health information is disclosed to a health plan for payment purposes.

DHHS covered health care components and internal business associates are required to take reasonable steps to correct any known material breach or violation of any business associate agreement. If such steps are unsuccessful, the agreement must be terminated, if feasible; and if not,

the problem must be reported to the DHHS Privacy Officer who will determine if further actions are warranted, which could include reporting the problem and correction attempts to the United States Department of Health and Human Services.

Should a covered health care component or internal business associate become a business associate of an agency external to DHHS, the Standard DHHS BAA must be utilized. Under no circumstances should any changes be made to this agreement without the express agreement of the Attorney General's office. If specific terms need to be addressed, they should be addressed in the contract, not the Business Associate Agreement.

Implementation

Identifying Internal and External Business Associates

Each agency that has at least one covered health care component or internal business associate must evaluate specific functions, activities, and services that are provided for, or on behalf of, that component/business associate to identify all internal and external business associates as follows:

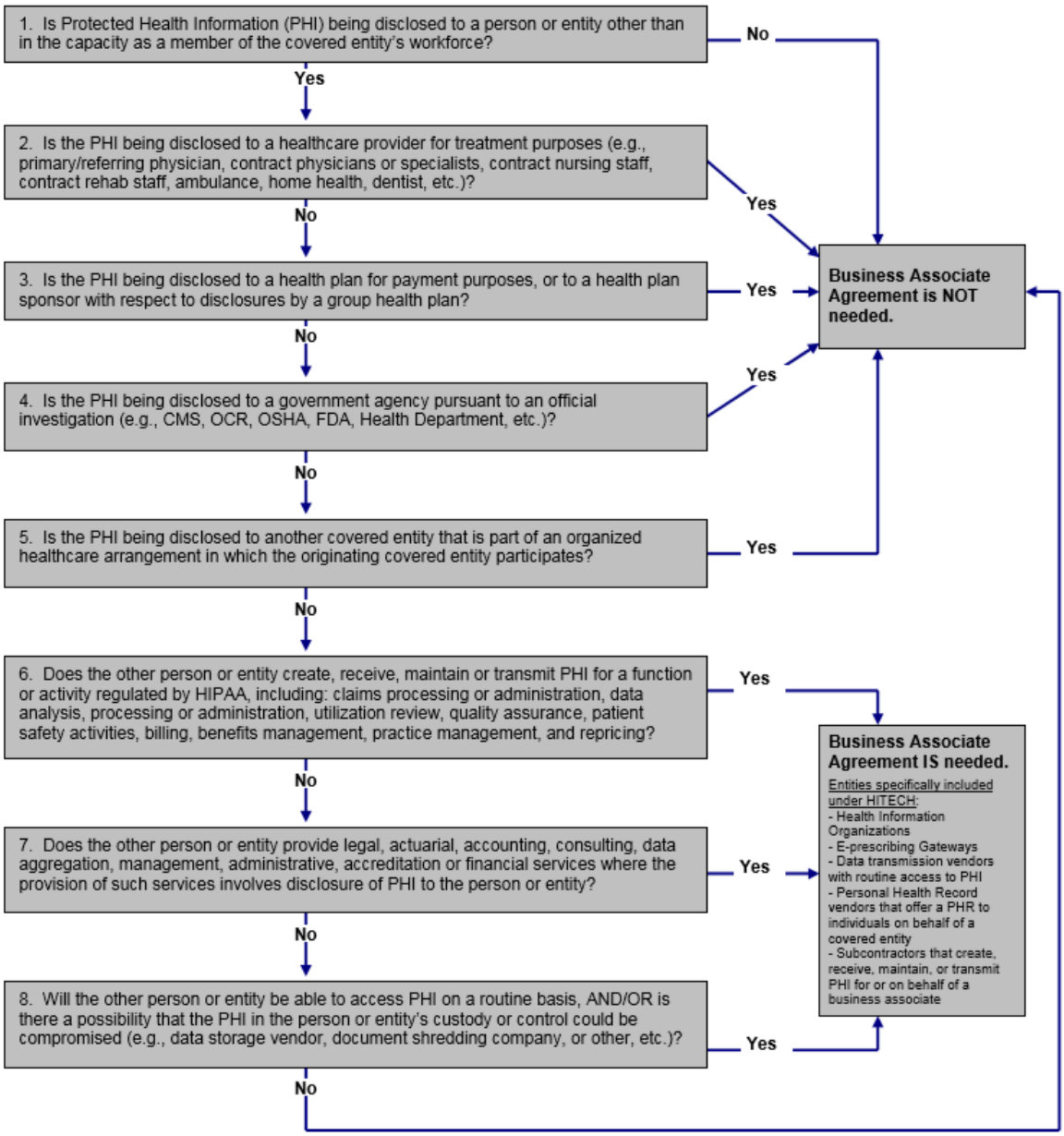
- Within the same DHHS division/office;
- Within other divisions in DHHS;
- Within other departments/agencies in NC state government; and
- Outside state government (external contractors).

Each agency must develop a process that identifies internal business associate relationships with other programs/units within the same division or with another division within DHHS. Components must maintain documentation of its internal business associates and update such information as internal business associates are added or deleted.

Each agency must also develop a process that identifies external business associate relationships at the time the agency initially creates a contract with the external contractor. Renewal of a contract that has a Business Associate Addendum requires a review of the Business Associate Agreement as well, for renewal purposes.

Covered components must identify all business associate relationships to standard contracts when entering contract information into the DHHS purchase and contracts database that monitors contracts. The Workgroup for Electronic Data Interchange (WEDI) has created a HIPAA/HITECH Business Associate Decision Tree to assist in making this determination**.**

HIPAA/HITECH
Business Associate Decision Tree



WEDI Privacy & Security Workgroup, Business Associate Sub-Workgroup Updated: July, 2013

Contractual Documentation Requirements

There are no Business Associate Agreement contractual documentation requirements for services provided by internal business associates, other than the agency's general documentation requirements.

Documentation of services provided by external contractors is accomplished through a DHHS standard contract. Documentation of business associate requirements is accomplished in an addendum to the contract. Business Associate agreements must be maintained for at least ten (10) years from the date of creation.

Only contract templates created by the NC Attorney General's Office should be used for business associate agreements. These documents include all of the updated HIPAA requirements to which their contractors must agree before covered health care components are allowed to share individually identifiable health information.

Beginning July 18, 2013, all new or amended DHHS contracts must be evaluated to determine whether a business associate relationship exists. If a business associate relationship does exist, a Business Associate Agreement must be in place. For HIPAA compliant BAAs executed prior to the publication of the Final Rule (1/25/13), the executed BAA may remain in effect until 9/22/2014, or such time as it needs to be revised, whichever comes first. If a new BAA needs to be created, it must be executed prior to September 23, 2013.

Termination of Business Associate Relationship

Should a DHHS covered health care component or internal business associate become aware of a pattern of activity, or practice of an internal business associate that constitutes a material breach or violation of the internal business associate's obligation with respect to privacy of individually identifiable health information in its possession, such information shall be forwarded to the DHHS Privacy Officer for resolution.

Should a DHHS covered health care component or internal business associate become aware of a pattern of activity or practice of an external business associate that constitutes a material breach or violation of the external business associate's obligations with respect to individually identifiable health information specified in a contract or other arrangement, reasonable steps should be taken to cure each breach, end the violation, and/or mitigate the consequences.

If such steps are unsuccessful, the covered health care component or internal business associate may, at its discretion:

- Terminate the contract or arrangement, if feasible; or
- If termination is not feasible, the agency privacy official is responsible for reporting the breach to the DHHS Privacy Officer. The DHHS Privacy Officer is responsible for resolution, which may include reporting the problem to the US DHHS Secretary at:

  Office for Civil Rights
  U.S. Department of Health & Human Services
  Atlanta Federal Center, Suite 3B70
  61 Forsyth Street, S.W.
  Atlanta, Georgia 30303-8909
  Phone: (404) 562-7886
  Fax: (404) 562-7881

Tracking of Business Associates

Each agency is required to track their internal business associates by maintaining current documentation of their internal business associates throughout the year.

DHHS agencies shall track their external business associates through the contracts that are entered into the department database for purchasing and contracts.

Training

DHHS covered health care components and internal business associates are not required to provide privacy training to their external business associates; nor are they required to monitor the privacy protections for individually identifiable health information that are instituted by their external business associates.

Reference

Department approved Business Associate Agreement template.

For questions or clarification on any of the information contained in this policy, please contact DHHS Privacy Officer For general questions about department-wide policies and procedures, contact the DHHS Policy Coordinator