

DPH Contract Review Process for HIPAA Privacy Impacts

Business Associate relationships and contract requirements are defined in the HIPAA Privacy Rule. Only HIPAA covered entities are subject to the provisions of the Privacy Rule, including BA requirements. In the case of DHHS, we are defined as a hybrid covered entity, which contains both covered and non-covered components within it. Non-covered components within a hybrid entity are not subject to the Privacy Rule.

Within the Division, the following are the only areas that are considered covered healthcare components and subject to the Privacy Rule provisions:

- State Lab
- Administrative, Local, and Community Support Section, HSIS Business Liaison
- Administrative, Local, and Community Support Section, Medicaid Reimbursement
- State Center for Health Statistics (pending review with AG's Office)
- Women and Children's Health Section, CY& Y Branch, Access to Care unit (HealthChoice)
- Women and Children's Health Section, CY& Y Branch, Specialized Services Unit (Children's Special Health Services)

Note that the CDSAs are covered by HIPAA because they bill Medicaid electronically, but are exempted from the Privacy Rule provisions because their records are protected by the Family Education Rights and Privacy Act (FERPA), which does not require business associate agreements

The following steps should be considered when reviewing contracts for HIPAA Privacy and business associate impacts:

1. Those contracts that we initiate from any of the above groups with other organizations that perform non-treatment related functions on our behalf AND that involve the use and disclosure of individually identifiable health information should be reviewed for potential HIPAA Privacy Business Associate relationships. These contracts should be reviewed with the HIPAA Office and if necessary with the AG's Office to determine whether a BA relationship exists.
2. Requests from external entities to enter into a business associate agreement with the Division should be forwarded to the HIPAA Office to review and prepare a response. These requests could result from our initiating a contract.
3. Confidentiality and protection of health information is part of our general contract terms and we can provide language that extends this if needed for specific grant/contract requirements. This requirement, however, is different than HIPAA business associate agreements, which are administratively very specific to the HIPAA Privacy Rule and who is covered. We want to ensure confidentiality per state and federal laws but do not want to create legal obligations under HIPAA where none exist.
4. If HIPAA Privacy BA relationship exists, we will need to include a business associate agreement addendum to the contract based on the approved DHHS HIPAA template. For inter-governmental agreements, we will need to either include the approved DHSS BAA addendum to an MOU or execute a standalone HIPAA BAA MOU based on the approved DHHS template.
5. The DHHS contracts database has been revised to include a field that indicates whether a BAA has been executed for a contract. DPH contracts management should update this field when a BAA has been executed.

Most of the confusion in general centers on the misconceptions that any exchange of identifiable health information constitutes a business associate relationship. However, A business associate relationship usually does not exist between providers for treatment-related services, a grantor and grant recipient, or payer and provider. Testing services provided by the lab for healthcare providers do not require a BAA since 1) they are treatment-related and 2) they are public health activities and are required by law. The business associate relationship most often exists when an entity provides other than healthcare services for the covered entity (covered component), such as legal, accounting, consulting, billing, utilization review services, among others.

Note: When we move to HIPAA Security, we will need to evaluate whether further types of business associate relationships will exist that extend beyond those defined for HIPAA Privacy.

Most of the DPH contracts should not require business associate review or agreements:

- The contracts are from Division unit not covered by the HIPAA Privacy Rule or
- The contracts are usually in the forms of grants to provide public health services
- The contract involves treatment services

Currently, we have one active business associate agreement in place with ValueOptions, performing medical review on behalf of HealthChoice special needs component for the Access to Care unit.

We have a stand-alone MOU with NCSU Student Health Services and the State Lab to provide lab-testing services, at NCSU insistence and against the AG's advice.

We have MOUs in place with DMA for SCHS and for Medicaid ALCSS Reimbursement unit. A BAA is not required between organizational units within the same covered entity (DHHS).

We have consolidated agreements with a BAA in place with the health departments for the ALCSS HSIS Business Liaison.

The HIPAA indicator field in the revised DHHS contracts database should be updated for ValueOptions to reflect that a BAA is in place. Any future BAAs for contracts should be updated. The contract database does not track MOUs.