TMA Privacy Office Information Paper

BA Contracts and Other Agreements

HIPAA Security ◆ November 2003

Standard Requirement

Business Associate Contracts and other Arrangements is one of the administrative safeguards that are required by the Security Rule. Under this standard, a covered entity may permit a business associate to "create, receive, maintain or transmit" electronic protected health information (EPHI) on its behalf. This can only be done if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information. (This standard replaces the "chain of trust" agreements in the proposed version of the rule.)When the covered entity and the business associate are both governmental entities, they may use a memorandum of understanding (MOU) in place of a contract.

The contract or other arrangement must require the business associate to do the following:

- Implement administrative, physical and technical safeguards that protects the electronic PHI that the business associate creates, receives, maintains, or transmits on behalf of the covered entity
- Ensure that any agents or subcontractors to whom the business associate provides information to will also implement safeguards to protect the information
- Report any security incidents to the covered entity
- Authorize termination of the contract if the covered entity finds that the business associate has violated the terms of the contract

Governmental agencies may delete the termination provision if it conflicts with the legal obligations of the business associate or covered entity. This ensures that health information that is protected by a provider, health plan or clearinghouse continues to be protected when given to someone that is not required to comply with HIPAA.

A covered entity that becomes aware of a violation of its contract or other arrangement must:

- take the necessary steps to end the violation;
- if those steps do not successfully end the violation, then the contract or arrangement must be terminated;
- if termination is not reasonable, the problem must be reported to the Department of Health and Human Services (DHHS)

DHHS has indicated that the covered entity is not required to examine every little detail of its business associates' activities. It can make assumptions about the good faith of those with whom and which it enters into contractual arrangements. A business associate

TMA Privacy Office Information Paper

BA Contracts and Other Agreements

is also not required to have the same level of security that exists at the covered entity. Rather, security must be reasonable and appropriate at each location and stage of its operations. Covered entities; however, are free to implement more demanding levels of security if they see fit. "This would be a business decision...." (Final Rule, p.8360)

Covered entities are not required to enter into new contractual or other arrangements to meet the Rule's requirements if existing written specifications already fulfill the Rule's minimum standards or can be amended to do so. (Final Rule, p.8360)

Implementation Specification
One required implementation specification exists with this standard, which is required:

Written Contract of Other Arrangement

Each covered entity must have written contracts and arrangements that meet HIPAA requirements. This emphasizes that the business associate contracts or other legal agreements must be in writing. The content of those agreements as required in this standard must be explicitly documented.

See also:
45 CFR 164.308(b)(1), 164.314(a)

Federal and DoD regulations that support this standard
OMB A-130 App. III
DoDI 8500.2