PRIVACY 27.0 BUSINESS ASSOCIATES AND BUSINESS ASSOCIATE AGREEMENTS

Scope: All subsidiaries of Universal Health Services, Inc., including facilities and UHS of Delaware Inc. (collectively, "UHS"), including UHS covered entities ("Facilities").

Purpose: To establish a policy: (i) requiring that prior to disclosing any PHI to a business associate of a Facility or allowing a business associate to create, receive, maintain or transmit PHI on its behalf, the Facility will obtain satisfactory assurances from the business associate that it will appropriately safeguard the PHI it receives or creates on behalf of the Facility; (ii) to provide guidance to Facilities in determining who is a business associate and on contracting with business associates; and (iii) to provide a template business associate agreement.

Definitions:

Terms not defined in this Policy or the *HIPAA Terms and Definitions* maintained by the UHS Compliance Office will have the meaning as defined in any related State or Federal privacy law including the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA") and regulations promulgated thereunder by the U.S. Department of Health and Human Services ("HHS") at 45 CFR Part 160 and 164, Subparts A and E ("Privacy Regulations" or "Privacy Rule") and Subparts A and C ("Security Regulations" or "Security Rule"), the Health Information Technology for Economic and Clinical Health Act ("HITECH") privacy and security provisions of the American Recovery and Reinvestment Act (Stimulus Act) for Long Term Care, Public Law 111-5, the American Recovery and Reinvestment Act of 2009 ("ARRA"), Title XIII and related regulations.

Policy:

Prior to disclosing any PHI to a business associate of a Facility or allowing the business associate to create, receive, maintain or transmit PHI, the Facility will obtain satisfactory assurances from the business associate that it will appropriately safeguard the PHI it receives or creates on the Facility's behalf. The Facility will document these satisfactory assurances in writing in the form of a business associate agreement ("BAA") that complies with HIPAA. A template BAA is attached to this Policy. Any disclosures to a business associates must be limited to disclosures permitted by the HIPAA regulations and not be made for their independent use or purposes.

Procedure:

A Facility may disclose PHI to a business associate, and/OR may allow a business associate to create, receive, maintain or transmit PHI on its behalf, only if: (i) the Facility obtains satisfactory assurances that the business associate will appropriately safeguard the PHI; and (ii)

the Facility documents these assurances by entering into a BAA with the business associate consistent with this Policy. The Facility must use the template BAA attached to this Policy as Attachment A, unless it obtains approval for a modification from the UHS Legal department. All requested revisions to the BAA must be approved by the UHS Legal department.

Determining Whether a Person or Entity is a Business Associate

As defined, a business associate is not a member of the Facility's workforce. A business associate generally is a person or entity:

> (1) that creates, receives, maintains, or transmits PHI for a covered entity in performing, assisting in the performance of, or providing a function or activity involving the use or disclosure of PHI, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, re-pricing, patient safety activities, peer review, and quality improvement;
>
> (2) that provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the covered entity, where the provision of the service involves the disclosure of PHI from the covered entity, or from another business associate of the covered entity, to the person or entity; or
>
> (3) that creates, receives, maintains or transmits PHI for any other function or activity regulated by HIPAA or its implementing regulations.

Another covered entity may be a business associate of the Facility. In addition, organizations such as Health Information Organizations, E-prescribing Gateways, Regional Health Information Organizations, or other organizations that provide data transmission of PHI and that require access on a routine basis to PHI are also business associates.

Examples of business associates include:

- A vendor providing patient billing or collection services
- A consultant reviewing the accuracy of billing and coding practices
- A company providing document shredding services to the Facility for the purpose of disposing PHI
- A person who provides medical transcription services for the Facility
- Companies that store documents or data containing PHI
- A Health Information Exchange to which the Facility provides PHI or allows access to PHI

- A vendor that contracts with the Facility to allow the covered entity to offer a personal health record to patients as part of the electronic health record

Examples of when no business associate relationship exists:

- Disclosures of PHI between the Facility and an outside health care provider for the purpose of patient treatment.

- Relationships with janitorial services companies, electricians, or certain construction workers, whose functions or services are not intended to involve the use or disclosure of PHI, and where any disclosure of PHI during the performance of their duties would be limited and incidental, such as disclosures that may occur while walking through or working in file rooms.

- A financial institution that processes consumer-conducted financial transactions by debit, credit, or other payment card, clears checks, initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or effects the transfer of funds for payment for health care. When it conducts these activities, the financial institution is providing its normal banking or other financial transaction services to its customers; it is not performing a function or activity for, or on behalf of, the Facility.

- An entity that functions as a mere "conduit" providing transportation or transmission services (digital or hard copy) – including entities providing only courier services, such as the US Postal Service, United Parcel Service, and electronic equivalents, such as internet service providers (ISPs) providing only data transmission services. (Such conduits transport information but do not access it other than on a random or infrequent basis as necessary to perform the transportation service or required by law).

- When none of the information disclosed is PHI, the person or entity receiving the information would not be a "business associate."

Disclosing PHI and/or Allowing Business Associates to Create, Receive, Maintain or Transmit PHI

Facilities may not disclose PHI to a business associate or allow a business associate to create, receive, maintain or transmit PHI on behalf of the until the Facility obtains satisfactory assurance that the business associate will appropriately safeguard the information as required by the HIPAA regulations, and that the business associate will ensure that any subcontractors that create, receive, maintain or transmit PHI on behalf of the business associate: (1) agree to comply with HIPAA and (2) enter into an appropriate business associate agreement. All of the other HIPAA requirements for business associates and BAAs must also be met. The Facility must enter into a BAA with each business associate in substantially the same format as the template

BAA in Attachment A. If the Facility modifies the attached template BAA, it must get approval from the UHS Legal department.

1. Minimum Necessary Applies

The Facility will disclose to a business associate only the PHI that is reasonably necessary to accomplish the intended purpose of the disclosure. Under a BAA, the business associate must request only the information that is the "minimum necessary," and therefore, the Facility may reasonably rely on a request from a business associate (or the business associate of another) to be a request for PHI that meets the minimum necessary standards. See UHS Privacy 6.0 *Minimum Necessary* for more information.

2. Limited Data Sets and Data Use Agreements

When a Facility discloses information to a business associate through the use of a "limited data set" pursuant to a data use agreement in accordance with UHS Privacy 7.0 *Limited Data Sets and Data Use Agreements*, a BAA would not be necessary for that disclosure.

Breach or Violation of Business Associate Agreement

If the Facility has actual knowledge of a material breach or violation of a BAA, or of a pattern of activity or practice of the business associate that constitutes a material breach or violation of a BAA (or other written contract evidencing the BAA), the Facility must take reasonable steps to cure the breach or end the violation, and if the steps are unsuccessful, the Facility Privacy Officer must:

- Work with the Facility contact for the business associate and the UHS Legal Department to terminate the underlying contract or arrangement with the business associate, if feasible;
- If termination of the underlying contract or arrangement with the business associate is not feasible, contact the UHS Legal department; and
- Mitigate, to the extent practicable, any harm effect that is known to the Facility arising from a disclosure of PHI in violation of the Facility's HIPAA policies and procedures and/or HIPAA.

Documentation

All BAAs (or other written contracts evidencing the BAA), should be signed on behalf of the Facility by the individual authorized to enter into the underlying contract for services. A copy of the executed BAA will be provided to the Facility Privacy Officer, for the purpose of maintaining a log of all BAAs entered into by the Facility. The Facility Privacy Officer will retain a copy of the BAA for (6) years after the contract expiration.

The Facility Privacy Officer will maintain a list of all active Business Associates. Attached as Attachment B: Business Associate Listing.

References:

45 C.F.R. 160.103
45 C.F.R. 164.502(e)
45 C.F.R. 164.504(e)
45 C.F.R. 164.524
45 C.F.R. 164.526
45 C.F.R. 164.528

Related UHS Policies:

UHS Privacy 7.0 *Limited Data Sets and Data Use Agreements*

UHS Privacy 6.0 *Minimum Necessary*

Attachment A: Template Business Associate Agreement

Attachment B: Business Associate Listing

Revision Dates:	**10-12-2017; 11-16-2015; 07-22-2013**
Implementation Date:	**07-25-2011**
Reviewed and Approved by:	**UHS Compliance Committee**