SECTION 3: USES & DISCLOSURES OF PHI

3.8 Business Associates and Vendors

POLICY

1. **Basis for Permission to Disclose Protected Health Information (PHI):** PHI maintained by the University of Florida (UF) may only be used by or disclosed to Vendors and Business Associates (BAs) who are specifically contracted to provide support services to UF that require the use or disclosure of PHI.
   
   a. Business Associate Agreements (BAAs) permit the use by, or disclosure of, PHI to such BAs and hold the BA accountable for safeguarding the PHI.
   
   b. BAAs must be in writing and must include terms authorized and approved by UF’s Privacy Office for maintaining compliance with federal privacy regulations.
   
   c. Use of an official UF BAA is preferred whenever possible.

2. **Scope:** It is the responsibility of each department, division, or operating unit within a designated health care component that is contracting for services with third parties where PHI will be used or disclosed, to ensure that contracts, service agreements, and purchase orders include the appropriate HIPAA-compliant verbiage, or that valid BAAs are executed.

3. **Business Associate’s Responsibility:** HIPAA standards, requirements, and implementation specifications that relate to privacy and security of PHI and that are applicable to Covered Entities (CEs) are also applicable to BAs (including the BA’s subcontractors) and shall be incorporated into any and all agreements between BAs and UF.

4. **Vendor Purchase Orders:** Certain purchases may be identified as potential opportunities for exposing PHI. Where no contract exists, but HIPAA-related implications apply for a general purchase, the Purchase Order will include the following statement, in lieu of a contract:

   VENDOR acknowledges that VENDOR may have access to protected health information (PHI) in various formats. VENDOR agrees to comply with all laws and policies covering security and confidentiality of PHI and to cooperate with the University of Florida’s monitoring of such compliance. VENDOR shall ensure that it will maintain all PHI in a secure and confidential fashion and that no PHI is disclosed to any third party except as permitted by law. VENDOR shall not disclose any PHI without first obtaining consent from the person to whom the record pertains or that person’s legal representative.

5. **UF’s Responsibility:** UF is responsible if it becomes aware of a pattern of activity or practice of a contracted vendor or BA that constitutes a material breach or violation of the Vendor's or BA's obligations. UF must take reasonable steps to cure the breach or end the violation, as applicable, and, if such steps are unsuccessful, terminate the contract or arrangement, if feasible;

**DEFINITIONS**

1. **Business Associate (HIPAA) means:**
   
   a. A person, not a member of the workforce, who:
      
      i. On behalf of a CE or of an organized health care arrangement (OHCA), creates, receives, maintains, or transmits PHI for a function or activity regulated by HIPAA, including claims processing or administration, data analysis, processing or administration, utilization review,
quality assurance, [certain] patient safety activities, billing, benefit management, practice management, and repricing; or

ii. Provides legal, actuarial, accounting, consulting, [certain] data aggregation services, management, administrative, accreditation, or financial services to or for such CE, or to or for an OHCA in which the CE participates, where the provision of the service involves the disclosure of PHI.

b. A covered entity may be a BA of another covered entity.

c. Business associate includes:

i. A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to PHI to a CE and that requires access on a routine basis to such PHI.

ii. A person that offers a personal health record to one or more individuals on behalf of a CE.

iii. A subcontractor that creates, receives, maintains, or transmits PHI on behalf of the BA.

d. Business associate does not include:

i. A health care provider, with respect to disclosures by a CE concerning the treatment of the individual.

ii. A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO) to the plan sponsor.

iii. A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting PHI for such purposes, to the extent such activities are authorized by law.

iv. A CE participating in an OHCA that performs a function or activity for or on behalf of such OHCA.

2. **Covered Entity (CE):** A health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered by the Privacy Rule.

3. **Subcontractor:** a person to whom a BA delegates a function, activity, or service, other than in the capacity of a member of the workforce of such BA.

4. **Vendor:** A person who provides goods or services. In a CE, the activities may involve direct, indirect, or incidental exposure to individually identifiable health information.

**PRIVACY REQUIREMENTS**

1. Compliance:

   a. A covered entity (CE) may disclose PHI to a BA and may allow a BA to create, receive, maintain, or transmit PHI on its behalf, if the CE obtains satisfactory assurance that the BA will appropriately safeguard the information.

   b. A CE may permit a BA to create, receive, maintain, or transmit electronic PHI on the CE’s behalf only if the CE obtains satisfactory assurances that the BA will appropriately safeguard the information.

   c. A CE is not required to obtain such satisfactory assurances from a BA that is a subcontractor.

2. Business Associate Contracts/Agreements:
a. The satisfactory assurances required above must be documented through a written contract or other written agreement or arrangement with the BA that meets the applicable HIPAA requirements, which are included in the approved UF BAA template.

b. BAA reviews are most often conducted by the following areas:
   a. UF Office of General Counsel (See Exhibits) or
   b. UF Purchasing Office.

REFERENCES

1. HIPAA: 45CFR §160.103 Definitions; §164.308(b) Administrative Safeguards - Standard: Business Associate Contracts; §164.314(a) Organizational Requirement – Standard: Business Associate Contracts; §164.502 Uses and Disclosures of PHI: General Rules; §164.504(e) Organizational Requirements

2. HITECH Act: Sec. 13401 (a) and 13404(a) (Application of Privacy Provisions and Penalties to Business Associates of Covered Entities); Sec. 13405 (c) (Accounting of Certain Protected Health Information Disclosures...)

EXHIBITS:

1. UF Office of General Counsel contact information at, http://generalcounsel.ufl.edu/contact-us/

2. UF Procurement at, https://procurement.ufl.edu/contracts/