HIPAA Guidance: When is a Third Party a Business Associate?

Introduction:

Use this guidance to determine if a third party that will have access to patient information is a "Business Associate," as the term is defined in the HIPAA regulations. Business Associates, or "BA"s must have a "Business Associate Agreement" (or "BAA") in place before they have access to patient information. The latest version of the BAA contains the name "UCMC BAA final 3" after the signature line on the last page. A copy can be found at http://hipaa.bsd.uchicago.edu/Current_BAA_UCMC_12102010.pdf.

> Subcontractors (known as downstream vendors) of Business Associates are also subject to HIPAA, but it is *our* Business Associate's responsibility to secure a Business Associate Agreement with its subcontactors.

When reviewing this guidance, keep in mind that the medical center means the hospital, the Biological Sciences Division, and the areas of the University that support patient care. These components together are called the "UC Organized Health Care Arrangement" or "UC OHCA." If you need assistance in determining if an area is within the UC OHCA, please contact the Privacy Program at 773-834-9716 or hpo@bsd.uchicago.edu.

Questions:

To determine if a third party is a Business Associate, review these questions.

1. Will the third party create, receive, maintain, transmit or use patient information? If the third party is not intended to create, see or use the patient information and the disclosure is incidental (e.g. a cleaning service), the person is not a Business Associate. However, the copy service does receive and maintain patient information (the information is contained in the machine's memory) and therefore is a Business Associate.

If yes, continue. If no, the third party is <u>not</u> a Business Associate.

2. Will the third party be providing services *to* or *acting on behalf of* the medical center (either the hospital and BSD)? A Business Associate is a person or entity that acts on the medical center's behalf related to a hospital function or activity.

If yes, continue. If no, the third party is <u>not</u> a Business Associate.

3. Is the person or entity:
   - a health care provider <u>and</u> the services involve treatment of the patient whose information is disclosed, or
   - within the UC OHCA (see the attached diagram).

If no, continue. If yes, the third party is <u>not</u> a Business Associate.

4. Does the third party fall within <u>any one</u> of the three following categories of Business Associates?

A. Does the third party perform or assist in the performance of a function or activity on behalf of the medical center? <u>The following are examples only, not an all inclusive list</u>:
    i. Claims processing or administration
    ii. Data analysis, processing or administration
    iii. Utilization review
    iv. Quality assurance
    v. Patient safety
    vi. Billing
    vii. Benefit management
    viii. Practice management
    ix. Repricing

B. Does the third party perform or assist in the performance of a function or activity for the medical center?

    Example: Any independent contractor retained by the medical center to assist with its implementation and enforcement of the HIPAA privacy or security standards <u>is</u> a Business Associate.

C. Does the third party provide any of the following services to or for the medical center?
    i. Legal
    ii. Actuarial
    iii. Accounting
    iv. Consulting
    v. Data aggregation
    vi. Management
    vii. Administrative
    viii. Accreditation
    ix. Financial

    It should be noted that the third category above (category (c)) is limited to the types of activities listed but the first category (category (a)) is <u>not</u> limited and is therefore potentially broader.

If yes to any of these, continue. If no, the third party is <u>not</u> a Business Associate.

5. Is the third party a health information organization, technology hosting platform, ePHI processor, or e-prescribing gateway (if the third party fits into this category, you must also engage the Information Security Office for a risk assessment):

If yes, continue. If no, the third party is <u>not</u> a Business Associate.

6. Does the third party fall within any one of these exceptions to Business Associate status:

A. Is the third party considered part of the medical center's "workforce" as defined by HIPAA?

"Workforce" is defined as employees, volunteers, trainees and others whose work is under the direct control of the covered entity, regardless of whether they are paid. The "direct control" requirement would exclude most independent contractors since tax and other rules generally require the covered entity to not assert any direct control over a contractor in order to avoid treatment as an employee.

- An example of a member of our workforce is our temporary nursing staff—the nurses are not Business Associates. However, the staffing company MAY be a Business Associate. The services the staffing company will provide will determine if it is a Business Associate.
- An example of someone who is not a member of our workforce is a consultant providing expertise in a certain area.

B. Is the third party merely a conduit for patient information without regular access to the information (e.g. not a facilitator of patient data transmission, such as an e-prescribing gateway)?

- A mere conduit, and therefore not a Business Associate, is the U.S. Post Office and Internet service providers.
- A facilitator of patient data transmission, which is a Business Associate, is a health information organization, an e-prescribing gateway, and a licensor of an electronic medical or other personal health record.

C. Is the third party a financial institution and its function is only to process consumer payments for healthcare?

If yes to any of these, the third party is not a Business Associate. Otherwise, the third party is a Business Associate.

When in doubt, call the Office of Medical Legal Affairs or the Privacy Program for assistance in understanding if a third party is a Business Associate.