STEP-BY-STEP PROCESS FOR DETERMINING WHETHER A BUSINESS ASSOCIATE AGREEMENT IS REQUIRED

A. INSTRUCTIONS

In accordance with HIPAA Privacy Policy #0017 – Business Associates, ECU staff shall use the following step-by-step process to determine whether a business associate agreement is required. Please proceed through this document step-by-step, beginning with Question #1. Reading any one question alone will not reveal whether a person or entity is a business associate.

B. DEFINITIONS

Except as otherwise defined below, any and all capitalized terms in this step-by-step process shall have the same definition provided in HIPAA Privacy Policy #0017.

Person - refers to the individual or entity (which may or may not be another covered entity) that is being evaluated to determine if that individual or entity is a business associate.

Subject - refers to the person who is the subject of health information (i.e., the individual that the health information is about).

You - any reference to "you" or "your" means an ECU Health Care Component and/or the Organized Health Care Arrangement in which a covered entity participates.

C. IS A BUSINESS ASSOCIATE AGREEMENT REQUIRED?

QUESTION # 1

Is the person a member of your Workforce?

If you answer "yes" to *both* of the following questions, the person is a member of your Workforce:

(a) Does the person perform work *on your behalf*?

(b) Do you have *direct control over the conduct* of the person when he or she performs work on your behalf?

- ❑ **If YES, STOP - the person is not a Business Associate. A Business Associate Agreement is not required.**
- ❑ **If NO, go to Question #2.**

QUESTION # 2

Do you disclose Protected Health Information (PHI) to the person who is a health care provider solely to allow the person or yourself to provide treatment to patients?

- ❑ **If YES, STOP - the person is not a Business Associate. A Business Associate Agreement is not required.**
- ❑ **If NO, go to Question #3.**

QUESTION #3

Do you disclose PHI to the person who is 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 protected health information for such purposes?

- ❑ **If YES, STOP - the person is not a Business Associate. A Business Associate Agreement is not required.**
- ❑ **If NO, go to Question #4.**

QUESTION #4

Do you disclose PHI to the person who is part of an Organized Health Care Arrangement with you and performs a function or activity, or provides a service, for or on behalf of such Organized Health Care Arrangement?

- ❑ **If YES, STOP - the person is not a Business Associate. A Business Associate Agreement is not required.**
- ❑ **If NO, go to Question #5.**

QUESTION #5

Does the person perform, or assist in the performance of, a function or activity, or provide a service that involves the use or disclosure of PHI?

Examples of a function or activity that may involve the use or disclosure of PHI include, but are not limited to, the following: (a) claims processing or administration, (b) data analysis, processing, or administration, (c) utilization review, (d) quality assurance, (e) patient safety activities[1], (f) billing, (g) benefit management, (h) practice management, and (i) repricing.

Examples of a service that may involve the use or disclosure of PHI include, but are not limited to, the following: (a) legal, (b) actuarial, (c) accounting, (d) consulting, (e) data aggregation[2], (f) management, (g) administrative, (h) accreditation, or (i) financial services.

- ❑ **If YES, go to Question #6.**
- ❑ **If NO, STOP. The person is not a Business Associate. A Business Associate Agreement is not required.**

QUESTION #6

Does the person (1) provide data transmission of PHI to you that (2) requires access on a routine basis [3]to such PHI?

[1] *Patient Safety Activities* means the following activities carried out by or on behalf of a PSO or a provider: (1) Efforts to improve patient safety and the quality of health care delivery; (2) The collection and analysis of patient safety work product; (3) The development and dissemination of information with respect to improving patient safety, such as recommendations, protocols, or information regarding best practices; (4) The utilization of patient safety work product for the purposes of encouraging a culture of safety and of providing feedback and assistance to effectively minimize patient risk; (5) The maintenance of procedures to preserve confidentiality with respect to patient safety work product; (6) The provision of appropriate security measures with respect to patient safety work product; (7) The utilization of qualified staff; and (8) Activities related to the operation of a patient safety evaluation system and to the provision of feedback to participants in a patient safety evaluation system. 42 CFR §3.20 (2012).

[2] *Data aggregation* means, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities. 45 CFR §164.501(2013).

[3] For more information regarding "access on a routine basis" please refer to *Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modification to the HIPAA Rules* 78 *Federal Register* 17 (23 January 2013), pp. 5571-5572 available online at http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

Examples of a person who may provide data transmission of PHI include, but are not limited to, the following: (1) health information organizations, or (2) e-prescribing gateways.

Examples of what it means to have access on a routine basis to such PHI include, but are not limited to, the following: (1) data or document storage companies, or (2) any entity with a persistent opportunity to access PHI.

- ❑ **If YES, go to Question #7.**
- ❑ **If NO, go to Question #8.**

QUESTION #7

Does the person fall under the conduit exception[4]?

The conduit exception is intended to exclude only those entities providing mere courier services or their electronic equivalent. Examples of entities that may provide this service include: (1) U.S. Postal Service or United Parcel Service, or (2) internet service providers.

- ❑ **If YES, STOP. The person is not a Business Associate. A Business Associate Agreement is not required.**
- ❑ **If NO, go to Question #8.**

QUESTION #8

Do you disclose PHI to a vendor that contracts with you to allow you to offer a Personal Health Record to patients as part of ECU's Electronic Health Record?

- ❑ **If YES, STOP. The person is a Business Associate. A Business Associate Agreement is required.**
- ❑ **If NO, go to Question #9.**

QUESTION #9

Does the person perform the functions or activities on your behalf?

NOTE: The phrase "on your behalf" is used in its common sense. Thus, an activity is performed on your behalf if, for instance, the person is acting as your representative, is acting for your benefit, and/or is acting in your interest and at your request.

- ❑ **If YES, STOP – the person is a Business Associate. A Business Associate Agreement is required.**
- ❑ **If NO, STOP – the person is not a Business Associate. A Business Associate Agreement is not required. [However, a confidentiality agreement may be required if PHI is being disclosed to an outside entity; please contact the ECU HIPAA Privacy Officer.]**

[4] For more information regarding the "conduit exception" please refer to *Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modification to the HIPAA Rules* 78 *Federal Register* 17 (23 January 2013), pp. 5572 available online at http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf