CHECKLIST: BUSINESS ASSOCIATES & WHEN A HIPAA BAA IS NEEDED

Identifying Business Associates

A HIPAA "Business Associate" generally is any person, other than a member of the workforce of a Covered Entity, who "***creates, receives, maintains or transmits***" **PHI** in the performance of ***services*** *or* ***functions*** **for** ***or*** **on behalf of** a Covered Entity. Business Associates may generally use and disclose a Covered Entity's PHI in order to perform and provide services and functions for and on behalf of a Covered Entity. A Business Associate may not use or disclose PHI in any manner which would violate HIPAA if done by a Covered Entity.

NOT HIPAA Business Associate Activities

"Treatment" activities do **not** create a Business Associate relationship, even if the other party receives PHI from a Covered Entity. Any disclosure made for treatment purposes to (i) a health care provider or (ii) another covered entity, is specifically excepted from the Business Associate standard. For example,

- A Covered Entity is not required to have a HIPAA Business Associate contract with the specialist to whom it refers a patient and transmits the patient's medical chart for treatment purposes.
- A physician is not required to have a HIPAA Business Associate contract with a laboratory as a condition of disclosing protected health information for the treatment of an individual.
- A Covered Entity laboratory is not required to have a HIPAA Business Associate contract to disclose protected health information to a reference laboratory for treatment of the individual.
- a Covered Entity may disclose protected health information needed for an orthopaedic device manufacturer or its representative to determine and deliver the appropriate range of sizes of a prosthesis for the surgeon to use during a particular patient's surgery.

"Payment" activities also do **not** create a Business Associate relationship where a Covered Entity is making the disclosure for its own payment purpose or for the payment purposes of another covered entity. Therefore, a Covered Entity may disclose PHI to a health plan in order to receive payment for services provided to a health plan's beneficiary.

Individuals with "**incidental access"** to PHI are also **not** considered Business Associates because they do not ***require*** access to or use of PHI in connection with performing their job functions. Therefore, contractors such as *electricians or plumbers, janitors, and security guards* are not considered Business Associates even if they may come into contact with PHI.

Likewise, entities which meet the test of a "**conduit"** are **not** Business Associates. The Office for Civil Rights ("OCR") and Department of Health and Human Services ("HHS") have traditionally recognized a limited ***exception*** to the business associate relationship for certain

entities that simply transport or transmit PHI. Entities such as the United States Postal Service, couriers, and their electronic equivalents transport but *do not have "**routine access**"* to PHI other than infrequently or randomly, and disclosure of the PHI to such entity is not intended.[1] These entities are treated as "conduits" through which PHI is transported, not HIPAA business associates.

The same conduit exception that applies to couriers, such as USPS and Fed Ex, also applies to their "electronic equivalents". As reiterated by the Preamble to the Final HITECH Rule,

> "The conduit exception is a narrow one and is intended to exclude only those entities providing mere courier services [*and their electronic equivalents*.] As we have stated in prior guidance, a **conduit transports information**, but **does not access it** other than on a random or infrequent basis as necessary to perform the transportation service or as required by other law." See 78 Fed Reg. 5571.

Thus, the occasional, random access by certain types of data transmission entity does not make the entity a business associate. The Preamble to the Final HITECH Rule gives the example of a telecommunications company which may have access to PHI when it reviews whether data being transmitted over its network is arriving to its intended destination. See 78 FR 5571-5572.

Conversely, an entity that **manages the exchange of PHI through a network**, including record locator services and various oversight and governance functions, **has more than "random access"** and would therefore meet the definition of a business associate. See 78 FR 5571. Furthermore, any entity that "**maintains PHI**" (i.e., provides data hosting of any kind) is a business associate *even if the entity does not actually access the PHI* given the persistent nature of that opportunity versus transient only. See 78 FR 5572.

Health Information Organizations (HIOs) and entities that act as health information service providers ("HISPs") can be treated as "conduits" and not business associates where the only services and functions they provide relate to data transmission or **routing of point-to-point encrypted** messages. According to the Direct Project[2] protocols, best practice standards, and related guidance for HISPs and secured health transport, a HISP which provides mere transmission or routing functions is not a business associate. Likewise, a HISP that transports only data that has already been encrypted by a sender and will remain encrypted until received by the intended recipient will not be a business associate unless it otherwise has access to unencrypted PHI on a routine basis or possess decryption keys or other mechanisms.

Therefore, there is **no** HIPAA business associate relationship implicated by an HIO, HISP or similar entity simply performing data transmission activities on behalf of a covered entity, akin to an internet cable provider. A business associate relationship **will**, however, be found where an HIO, HISP or similar entity performs more than just mere data transmission, such as

[1] See www.hhs.gov/ocr/privacy/hipaa/faq/smaller_providers_and_businesses/245.html.

[2] The DIRECT Project is a federal and stakeholder initiative aimed at establishing standards and documentation to support sending encrypted health data and messages to known recipients. See http://directproject.org/home.php.

data aggregation, processing, hosting and transmission (other than as a conduit), encryption/decryption functions, record locator/querying functions, auditing and other oversight and governance functions, and creating data sets of de-identified information.[3] These activities trigger HIPAA business associate obligations, including compliance with applicable provisions of the HIPAA Security Rule, written security policies and procedures, and written BAAs, among others.

HIPAA Business Associate Activities

Business Associate Activities include information technology support teams, software vendors and the like who provide support to a Covered Entity's electronic medical records where they require access to, create, maintain or transmit PHI in order to perform functions and services on behalf of a Covered Entity. Likewise, a medical malpractice defense law firm, consultants who assist with utilization reviews, or medical transcriptionists, are persons who would be considered Business Associates where they require access to PHI in order to perform functions on behalf of a Covered Entity. Other examples include,

- Claims processing, billing, data analysis and processing, quality assurance, and practice or benefits management;
- Legal, accounting, financial, consulting, management, support and accreditation activities;
- Health IT and similar vendors that provide security support, data hosting and data backup (i.e., electronic medical record vendors) and patient personal health record vendors (PHRs);
- Health Information Exchange Organizations that facilitate electronic transmission of PHI and require "routine access" to such information, or which maintain PHI, even if they do not view it.

[Business Associate Identification Tool continues on next page]

[3] See 45 CFR § 160.103; § 164.103.

Legal Health information eXchange™

Business Associate Identification Tool

Step 1. Determine whether vendor or contractor is providing services to or on behalf of a Covered Entity:

- ☐ There is a **contract** or other **arrangement** through which an entity performs a function, service or activity *for or on behalf of* a Covered Entity. *Go to Step 2.*

- ☐ There is a contract or agreement, but the entity does not perform a function, service or activity *for or on behalf of* a Covered Entity. **STOP**. *This is not a Business Associate and a HIPAA BAA is not required. Another form of confidentiality or data use agreement may be required if entity would have access to a Covered Entity PHI and the access would not fit within HIPAA permitted uses or disclosures.*

Step 2. Determine whether vendor or contractor will have access to, create, maintain or transmit a Covered Entity data in the course of providing such services:

- ☐ Entity **requires or may require** access to some or all of a Covered Entity data in order to perform contractual services for a Covered Entity or otherwise may **create, receive, transmit or maintain** a Covered Entity PHI. *Go to Step 3.*
  - This includes PHRs, EMRs, HIOs, and other vendors that access, host or facilitate electronic transmission of PHI and which may have (1) **routine access** to such data or (2) **maintain data**, even if they do not view it other than randomly or infrequently.

- ☐ Entity may have access, but access would not be routine and would only be **incidental** to performance of services (i.e., janitorial contract staff, contract security guards, or Couriers, U.S. Postal Service, United Parcel Service, telecommunications providers, and similar entities with random or infrequent access that are mere "conduits" for PHI). **STOP**. *This is not a HIPAA Business Associate and a HIPAA BAA is not required. Another form of confidentiality agreement may be required.*

- ☐ Entity does not require and will not have access to any of a Covered Entity data in order to perform contractual services for a Covered Entity. **STOP**. *This is not a HIPAA Business Associate and HIPAA BAA is not required. Another form of confidentiality agreement may be required.*

Step 3. Determine what **type** of a Covered Entity data the vendor or contractor needs access to, wants or will otherwise be responsible for:

- ☐ **Individually Identifiable** ("PHI") – (See a Covered Entity HIPAA Policies) *Go to Step 4.*
  - Information that includes demographic information of an individual and (1) is created or received by a Covered Entity) and (2) relates to the past, present or future physical or mental health or condition of an individual, the provision of care to an individual, or the past, present or future payment for the provision of health care to an

individual and that (i) identifies the individual or (ii) for which there is a reasonable basis to believe the information can be used to identify the individual.

- **PHI includes but is not limited to**: (1) Names, (2) Dates relating to an individual such as birth date, admission/discharge date, (3) Telephone, fax or email, or (4) social security numbers, medical record or health plan beneficiary numbers.

☐ **Other a Covered Entity data** (i.e., accounting, legal, business, employee (non-health plan related) and others). **STOP**. *This is not a HIPAA Business Associate and a HIPAA BAA is not required. Other form of confidentiality agreement may be required.*

☐ **Both Individually Identifiable (PHI) and other a Covered Entity data.** *Go to Step 4.*

Step 4. Determine the **purpose** for which the information is sought (i.e., treatment, research, or health care operations of a Covered Entity)

☐ Treatment or research activities. *This is* **not** *a HIPAA Business Associate. If for research activities, please refer to a Covered Entity's HIPAA "Research" Policy for use/disclosure of PHI in the research context.*

☐ Payment-***related*** activities. (i.e., claims **review**, billing management and administration ***for or on behalf of*** a Covered Entity) **THIS IS A BUSINESS ASSOCIATE.**

☐ Other a Covered Entity health care operations and other activities. (i.e., accreditation entities, attorneys litigating malpractice claim, cloud-based vendor storing electronic PHI, health plan administrator accessing employee health plan information) **THIS IS A BUSINESS ASSOCIATE.**

[BAA Checklist continues on next page]

Legal Health information eXchange™

Business Associate Agreement Checklist

A HIPAA Business Associate Agreement (HIPAA BAA) is required *prior to* disclosing any PHI to a third party vendor or other contractor who is performing functions or services for or on behalf of a Covered Entity (i.e., billing, data hosting) and which requires or may create, receive, maintain or transmit PHI in connection with such ("Business Associates").

- ❑ Use a Covered Entity's standard "HIPAA Business Associate Agreement" (HIPAA Vendor BAA). **This form should be used for any entity performing services for a Covered Entity who requires access to, use or disclosure of PHI in the performance of such services, including where such vendor is maintaining PHI for a Covered Entity (i.e., cloud-based servers).**

- ❑ Review Services Contract with vendor to identify need to access, use or disclose PHI to perform contracted functions and services and tailor HIPAA Vendor BAA to appropriately reflect uses and disclosures of PHI which vendor may engage in under the Services Contract.

- ❑ A HIPAA BAA must at a minimum:

  - ☐ It must **spell out** the permitted & required uses and disclosures of the PHI by the BA

  - ☐ It cannot authorize or allow the BA to use or further disclose the PHI in any manner that would violate the requirements of the Privacy Rule if done by a Covered Entity, except may permit use and disclosure for BA's management and administration or BA's legal responsibilities as described below.

  - ☐ It must state that the BA will:
    - Not use or further disclose the information other than as permitted or required by the HIPAA BAA, or as required by law
    - Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the underlying Agreement
    - Report to a Covered Entity any use or disclosure of the information not provided for by its contract of which it becomes aware, including any Security Incidents or Breaches of Unsecured PHI,
    - **Ensure that any subcontractor to whom it provides PHI received from, or created or received by the BA on behalf of a Covered Entity, agrees in writing to the same restrictions and conditions that apply to the BA (i.e., HIPAA BAA between the BA and subcontractor)**
    - Make available PHI in accordance with HIPAA access rights, § 164.524
    - Make available PHI for amendment and incorporate any amendments to PHI in accordance with HIPAA at § 164.526
    - Make available information required to provide an accounting of disclosures in accordance with HIPAA at § 164.528
    - Make available its internal practices, books and records relating to the use and disclosure of a Covered Entity's PHI to the Secretary for purposes of determining a Covered Entity's compliance

- Give authority to a Covered Entity to terminate, where it becomes aware of a pattern of activity or practice of the BA that constitutes a material breach or violation of the HIPAA BAA, to terminate the HIPAA BAA or underlying arrangement.
- For e-PHI, comply with the Security Rule and implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of that e-PHI that it creates, receives or maintains or transmits on behalf of a Covered Entity

☐ The HIPAA BAA should also include a Covered Entity's standard security breach notification provisions, including timeframes for notice, as included in a Covered Entity's HIPAA Vendor BAA

☐ The HIPAA BAA ***may,*** but is not required to, ***permit*** the BA to:

- Provide data aggregation services relating to a Covered Entity's health care operations;

- **Use** PHI received in its capacity as a BA, if necessary for the proper *management and administration of the BA*, or to carry out legal responsibilities of BA;

- **Disclose** the information received in its capacity as a BA for the proper management and administration of the BA, or to carry out the legal responsibilities of the BA **IF:**

  ☐ The disclosure is required by law; or

  ☐ BA obtains reasonable assurances from the person to whom the PHI is disclosed that it will:

    ☐ be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and

    ☐ the person notifies the BA of any instance of which it is aware in which the confidentiality of the information has been breached.