Washington State Department of Social & Health Services

Transforming lives

Administrative Policy No. 13.23

Subject:	Identifying Business Associates and Business Associate Agreements
Information Contact:	Central Contracts & Legal Services, MS45811
Authorizing Source:	DSHS Administrative Policy 5.01, Privacy Policy -- Safeguarding Confidential Information DSHS Administrative Policy 5.03, Client Rights related to Protected Health Information DSHS Administrative Policy 5.06, Use and Destruction of Health Care Information DSHS Administrative Policy 13.10, Central Contracts & Legal Services DSHS Administrative Policy 13.11, Monitoring Contractor Performance DSHS Administrative Policy 13.08, Operational (Purchased) Goods and Services HIPAA Rules – 45 CFR Parts160, 162, and 164 HITECH Act
Effective Date:	March 3, 2015
Revised:	June 24, 2019
Approved By:	**ORIGINAL SIGNED BY Mark Eliason** Senior Director for Policy and External Relations

Purpose

To establish guidelines for Department of Social and Health Services (DSHS) to identify those relationships with vendors and other entities that meet the definition of a "business associate" under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, and to provide direction in establishing formalized business associate agreements. DSHS shall implement the required procedures and ensure documentation to establish satisfactory assurance of compliance. HIPAA requirements for business associates are addressed in the following federal regulations:

- 45 CFR 164.308(b)(1)–(3) – HIPAA Security Rule Administrative Safeguards Business Associate Contracts and Other Arrangements

- 45 CFR 164.314 – HIPAA Security Rule Organizational Requirements Business Associate Contracts or Other Arrangements
- 45 CFR 164.502(e)(1) – HIPAA Privacy Rule Uses and Disclosures of Protected Health Information: General Rules – Disclosures to Business Associates
- 45 CFR 164.504 – HIPAA Privacy Rule Uses and Disclosures: Organizational Requirements

These regulations define the concept of a business associate relationship and outline the required elements to be included in a business associate agreement. This policy, and any procedures or guidelines referenced, is intended for internal use only. This policy is not intended, nor can it be relied upon, to create any substantive or procedural rights enforceable by any party involved in matters with DSHS.

Background

HIPAA requires that all organizations subject to its provisions prevent unauthorized access to "protected health information" or PHI. PHI includes patients' or clients' names, addresses, and all information pertaining to their health and payment records. HIPAA, as amended by the Health Information Technology for Economic and Clinical Health Act, and as incorporated in the American Recovery and Reinvestment Act of 2009 ("HITECH"), has a number of components including the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule"), Notification in the Case of Breach of Unsecured Protected Health Information ("Breach Notification Rule"), and the Security Standards for the Protection of Electronic Protected Health Information (the "Security Rule") found at Title 45, Parts 160 and 164 of the Code of Federal Regulations (CFRs). Collectively, these regulations are referred to in this policy as the HIPAA Rules. HITECH requirements were implemented by the U.S. Department of Health and Human Services via the Omnibus Rule, which became effective on September 23, 2013.

The HIPAA rules apply to "covered entities" and "business associates," as those terms are defined by 45 CFR 160.103. Individuals, organizations, and agencies that meet the definition of a covered entity under HIPAA must comply with the requirements of the rules to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information. If a covered entity engages a business associate to help it carry out its health care activities and functions, the covered entity must have a written business associate contract with the business associate that establishes specifically what the business associate has been engaged to do and requires the business associate to comply with the Rules' requirements to protect the privacy and security of protected health information. In addition to these contractual obligations, business associates are directly liable for compliance with certain provisions of the HIPAA Rules.

The HIPAA Privacy Rule provides federal protections for individually identifiable health information held by covered entities and their business associates and gives individuals a number of rights with respect to that information. At the same time, the Privacy Rule is balanced so that

it permits the disclosure of health information needed for patient and client care and other important purposes.

The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to assure the confidentiality, integrity, and availability of electronic protected health information. Complete compliance with HIPAA rules requires implementation of security measures. Please refer to the DSHS Information Security Standards Manual, DSHS Information Security Procedures Manual, and DSHS Administrative Policy 5.01 regarding required security measures for protected health information within the Department.

If an entity does not meet the definition of a covered entity or business associate, it does not have to comply with the HIPAA rules. See definitions of "business associate" and "covered entity" at 45 CFR 160.103. Refer to Appendices 1 and 2 of this administrative policy for guidance in determining who is and who is not a DSHS "business associate."

Scope

This policy applies to all health care components of DSHS involved with external entities meeting the definition of "business associate." DSHS is a hybrid covered entity which has designated certain programs within the administrations and divisions as health care components as provided in DSHS Administrative Policy 5.01. DSHS health care components are listed on the DSHS website. As a hybrid covered entity, only DSHS health care components are subject to the HIPAA rules. Areas that are deemed non health care components are not subject to the HIPAA rules.

The health care components of DSHS are required to sign business associate agreements with certain organizations and individuals with whom they share protected health information. Business associates are outside organizations, entities, and individuals who perform some function or service for the health care components that requires them to have access to our client's protected health information.

Definitions

Agency contracts database (ACD). The ACD is the system used by DSHS for producing, tracking, and monitoring all DSHS personal service, client service, purchased service, interlocal (interagency) and intergovernmental contracts and agreements. See DSHS Administrative Policy 13.10.

Business associate (BA): A person who, on behalf of DSHS other than in the capacity of a member of the workforce, performs a function or activity involving the use or disclosure of Protected Health Information (PHI) to carry out essential functions or perform services for DSHS. "Business Associates" include subcontractors who create, receive, maintain or transmit PHI on behalf of a primary Business Associate.

Business associate agreement (BAA): Under the HIPAA Privacy and Security Rules, a legally binding agreement entered into by a covered entity and business associate that establishes

permitted and required uses and disclosures of protected health information (PHI), provides obligations for the business associate to safeguard the information and to report any uses or disclosures not provided for in the agreement, and may require termination if violated.

Business associate organizational units (BAOU): BAOU's are internal to DSHS and perform the department's daily activities that relate to providing health care. These activities must relate to covered functions. Some examples of covered functions include: conducting quality assessment and improvement activities; case management and care coordination; contacting of health care providers and patients or clients with information about treatment alternatives; legal, actuarial, accounting, consulting, data aggregation, management administrative, accreditation, or financial services; and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits.

Central contracts and legal services (CCLS). CCLS means the statewide DSHS headquarters contracting office in the services and enterprise support administration.

Contract manager. The contract manager is the individual assigned in the ACD as the person primarily responsible for the day-to-day management activities related to contracting out services, including contractor screening, contractor selection, contract preparation, and monitoring contractor performance. See DSHS Administrative Policy 13.10.

Covered entity: A covered entity is a health plan, a health care clearinghouse, or a health care provider. A health care provider is a covered entity if it transmits information electronically in conjunction with a HIPAA standard transaction (see 45 CFR 160.103). DSHS is a hybrid covered entity that has designated programs as health care components within the administrations and divisions as provided on the DSHS Website. As a hybrid covered entity only its Health Care Components are subject to the HIPAA rules.

Electronic protected health information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Health care component (HCC): A component or combination of components of a hybrid covered entity designated by the hybrid covered entity as a health plan, a covered health care provider, or both. This includes the business associate organizational units (defined above).

HIPAA: The Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d et seq. To implement HIPAA, the U.S. Department of Health and Human Services Office for Civil Rights (OCR) has adopted the HIPAA Privacy Rule, Security Rule, and Breach Notification Rule.

HIPAA Rules: References to the "HIPAA Rules" mean the rules that OCR enforces and includes the HIPAA Privacy Rule, for protecting the privacy of individually identifiable health information; the HIPAA Security Rule, setting national standards for the security of electronic protected health information; the HIPAA Breach Notification Rule, requiring covered entities and business associates to provide notification following a breach of unsecured PHI; and the

confidentiality provisions of the Patient Safety Rule, protecting identifiable information being used to analyze patient safety events and improve patient safety.

Hybrid covered entity: A single legal entity that is a covered entity whose business activities include both covered and non-covered functions; and that designates HCCs in accordance with the Privacy Rule. See 45 CFR 164.103 and .105. DSHS is a hybrid covered entity under the HIPAA Privacy Rule.

Key contract coordinator. Key contract coordinator means the individual(s) designated by the division director responsible for contracting in a given Administration to be the liaison between the administration and CCLS. The key contract coordinator has specific, direct responsibilities for DSHS contracting processes that are identified in DSHS Administrative Policy 13.10.

Non-health care component (Non-HCC): A component or combination of components of a hybrid covered entity that is not subject to HIPAA Rules.

Organized health care arrangement (OHCA): An arrangement or relationship recognized in the HIPAA Privacy Rule that allows two or more covered entities who participate in joint activities to share protected health information (PHI) about their patients or clients in order to manage and benefit their joint operations.

Protected health information (PHI): Individually identifiable health information about a client that is transmitted or maintained by a DSHS health care component in any form or medium. PHI includes demographic information that identifies the individual or about which there is reasonable basis to believe can be used to identify the individual. Individually identifiable health information in DSHS records about an employee or others who are not clients is not protected health information. See DSHS Administrative Policy 5.03 for provisions relating only to PHI of clients.

Required Procedures:

1. The responsibilities related to the management of BA relationships and agreements for health care components and business associate organizational units are delegated as follows:

a. **Central contracts & legal services (CCLS).** CCLS is responsible for drafting and keeping up to date the DSHS standard BA language. CCLS is also responsible for determining exceptions to the standard business associate language.
b. **Chief information security officer.** The chief information security officer is responsible for approving any exceptions to DSHS standard data security requirements language. See Information Security Policy Manual, Section 3.2.4.
c. **Programs.** Contract managers and key contract coordinators are responsible for ensuring appropriate data security requirements language is also included in any contract that includes business associate language.
d. **Privacy officer.** The privacy officer may be consulted regarding use of, and requested exceptions to, the DSHS standard business associate language.

2. Contract managers and key contract coordinators are responsible for facilitating the assessment of all DSHS contract relationships to determine whether the contractual relationship meets the criteria for a HIPAA business associate agreement (See Appendix 1 for general guidance as to types of vendors and businesses that would or would not be considered business associates). The following criteria define a Business Associate under HIPAA:

a. The vendor or business' staff members are not members of the Department's workforce.
b. The vendor or business is doing something on behalf of the Department;
c. That "something" involves either the use, or disclosure of PHI, or both.
d. Note that there are certain disclosures to vendors and businesses that do not require establishment of a BAA (see 45 CFR 164.502(e)(1)). These disclosures include:
   (1) Disclosures by a covered entity to a health care provider concerning the treatment of the individual;
   (2) Disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that the requirements of 45 CFR 164.504(f) apply and are met; or
   (3) Uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the PHI used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.

3. Contract managers and key contract coordinators should determine the need for BAAs through:

a. Mapping the flow of PHI and identifying where PHI is used or disclosed or created by external entities.
b. Reviewing contract documents and identifying where PHI is disclosed to external entities.
c. Assessing new contractor or vendor business arrangements to determine if PHI will be used or disclosed, documenting these decisions using the checklist in Appendix 2 and retaining such documentation in the contract file.
d. Consultation with CCLS as needed.

4. When it has been determined that a BA arrangement exists, the contract manager and key contract coordinator must ensure a BAA is entered into using the DSHS standard BA language developed and maintained by CCLS. The contract manager and key contract coordinator must ensure the contract includes the preapproved HIPAA compliance language by selecting the appropriate "HIPAA" designated contract code in the ACD at the time the contract is created. If a service or purchase is being made under a Department of Enterprise Services (DES) master contract under circumstances that amount to a BA arrangement, either the ordering document must include the appropriate

BA language, or a separate standalone BAA must be entered into with the vendor or contractor.

5. Due to HIPAA compliance tracking requirements, simply attaching a BAA to a contract as an exhibit is not a satisfactory method of meeting the requirements of this policy. If it is not possible to include the BAA by selecting the "HIPAA" designated contract code in the ACD at the time of contract creation (e.g., if entering into an interlocal agreement using the other party's form of agreement or some other form of "outside the agency" contract), DSHS must execute a separate standalone BAA with the vendor or contractor and that BAA must be separately recorded in the ACD.

6. If a business associate reports privacy breaches or security incident events as required by the agreement, please refer to DSHS Administrative Policy 5.01 (Safeguarding Confidential Information).

7. All DSHS business associate agreements must be maintained in the ACD as required by DSHS Administrative Policy 13.10.

8. All BAA documentation shall be maintained for a period of six years beyond the date the BA relationship is terminated. See chapter 40.14 RCW for the applicable records retention requirements.

9. The BAA shall be effective for the length of the relationship between DSHS and the BA organization, unless otherwise terminated under the provisions outlined in the agreement.

APPENDIX 1: Examples of Business Associates

EXAMPLES OF BUSINESS ARRANGEMENTS THAT MAY INVOLVE DISCLOSURE OF PHI & REQUIRE BA AGREEMENTS/HIPAA LANGUAGE	
Accrediting/Licensing Agencies (JCAHO) Accounting Consultants/Vendors Actuarial Consultants/Vendors Agents/Contractors Accessing PHI (Consultants) Application Service Providers (i.e., prescription mgmt.) Attorneys/Legal Counsel Auditors Benchmarking Organizations Benefit Management Organizations Claims Processing/Clearinghouse Agency Contracts Coding Vendor Contracts Collection Agency Contracts Computer Hardware Contracts Computer Software Contracts Consultants/Consulting Firms Data Analysis Consultants/Vendors Data Warehouse Contracts Emergency Physician Services Contracts Hospitalist Contracts Insurance Contracts (Coverage for Risk, Malpractice, etc.) Interpreter Services Contracts IT/IS Vendors Legal Services Contracts Medical Staff Credentialing Software Contracts Microfilming Vendor Contracts Optical Disc Conversion Contracts Pathology Services Contracts Paper Recycling Contracts Patient Satisfaction Survey Contracts	Payer-Provider Contracts (Provider for Health Plan) Physician Billing Services Physician Contracts Practice Management Consultants/Vendors Professional Services Contracts Quality Assurance Consultants/Vendors Radiology Services Contracts Record Copying Service Vendor Contracts Record Storage Vendors Release of Information Service Vendor Contracts Repair Contractors of Devices Containing PHI Revenue Enhancement/DRG Optimization Contracts Risk Management Consulting Vendor Contracts Shared Service/Joint Venture Contracts with Other Healthcare Organizations Statement Outsource Vendors Telemedicine Program contracts Third Party Administrators Transcription Vendor Contracts Waste Disposal Contracts (Hauling, Shredding, etc.) **Health Plan Relationships:** Pharmaceutical Benefits Management Contracts Preauthorization Management Contracts Case Management Contracts Third Party Administrator (TPA) Contracts Wellness Promotion Contracts

EXAMPLES OF BUSINESS ARRANGEMENTS THAT MAY INVOLVE DISCLOSURE OF PHI & REQUIRE BA AGREEMENTS/HIPAA LANGUAGE	
EXAMPLES OF ARRANGEMENTS THAT ARE USUALLY NOT BUSINESS ASSOCIATE RELATIONSHIPS AND MAY NOT REQUIRE BA AGREEMENTS/HIPAA LANGUAGE	
Banks Processing Credit Card Payments Blood Bank/Red Cross (Provider) Clinics (Provider Relationships) Courier Services Delivering Specimens Device Manufacturers that Require PHI to Produce Pacemakers, hearing aids, glasses, etc. (Treatment) Cleaning/Janitorial Services Durable Medical Equipment (DME) for Treatment Purposes Educational/School Programs (Student Privacy Education Required as Workforce Member) Health Plans Contracting With Network Providers (Covered Entity to Covered Entity) Health Plans for Purposes of Payment Hospitals Housekeeping/Environmental Services (Incidental Exposure) Infusion Provider for Treatment Members of an Affiliated Covered Entity Members of the Organization's Organized Health Care Arrangement (OHCA) Pharmacy (Healthcare Provider/Treatment) Providers (Involved in Care, Treatment, or Services to DSHS Clients)	Members of the Organization's Workforce Organ Procurement Organizations Nursing Homes Rental Employee Agencies (No PHI Shared – Employees Need Privacy Training) Repair Contractors (Maintenance, Copy Machine, Plumbing, Electricity, etc. – No PHI involved) School Health Nurses Supply Services Support Services Agreements for Supplies/Treatment Purposes Tissue Banks USPS, FedEx, and Other Common Carriers Volunteers (Board Members, Ethics Committee Members, Institutional Review Board, etc.)

APPENDIX 2: CHECKLIST FOR DETERMINING BUSINESS ASSOCIATES

CHECKLIST FOR DETERMINING BUSINESS ASSOCIATES

ACD Contract Number: _____
Date Signed: _____
Reviewer: _____

Common examples of business associate relationships include:

- Coding and billing provider
- Waste disposal and recycling company
- Medical transcription service
- Microfilm, optical disk conversion provider (or any other archiving)
- Clearinghouse
- Billing company
- Insurance broker or insurance company
- Records management company (storage and reproduction)
- Temporary staffing agency
- Software and hardware provider who accesses PHI for installation, maintenance and support services
- Implant vendor
- Other medical/surgical vendor with representatives on site who perform a function or activity for or on behalf of DSHS.
- On-site service provider for medical equipment/instrumentation where exposure to PHI would be more than incidental
- Lawyers, Accountants, Consultants, Independent Contractors with access to PHI

Reviewers are also directed to Appendix 1 of Administrative Policy No. 13.23 for guidance in determining who is and who is not a "business associate."

1. What type of business is the vendor? _____

2. Does the vendor perform a function, service or activity (on our behalf) that uses/discloses Protected Health Information (PHI)?

_____ Yes, go to #3.
_____ No, this is not a Business Associate.

3. Does the PHI used/disclosed include any of the following fields?

- Name
- Street address
- Telephone or fax numbers

- E-mail
- Social Security Number
- Certificate/License Numbers
- Vehicle identifiers and serial numbers
- URL's and IP addresses
- Face photographs or any comparable images
- Any other unique identifying number, characteristic, or code (which includes the DSHS Client Identification Number)
- Device identifiers and serial numbers
- Biometric identifiers, including fingerprints and voiceprints.

_____ Yes, go to #4.
_____ No, this is not a Business Associate, but a Data Sharing/Usage Agreement should be signed.

4. Are the individuals getting access to PHI on behalf of the vendor outside our workforce (not employees, volunteers, trainees, etc.)? (Workforce means employees, volunteers, trainees, and other persons who perform work for a covered entity under the direct control of such covered entity, whether or not they are paid by the covered entity).

_____ Yes, go to #5.
_____ No, this is not a Business Associate.

5. Is the service for treatment (services to or for patients by healthcare providers)?

_____ No, go to #6.
_____ Yes, this is not a Business Associate.

6. Is the vendor:

(a) A government agency with medical staff privileges to treat patients;
(b) A health plan where PHI is disclosed for enrollees of the plan; or
(c) A person with medical staff privileges to treat patients?

_____ No, go to #7.
_____ Yes, this is not a Business Associate.

7. Is the vendor acting as a mere conduit of PHI (USPS, Fed-Ex, UPS, etc.) or a financial institution? A conduit is a vendor that does not store PHI.

_____ No**, this vendor is a Business Associate.** Utilize the HIPAA contract language.
_____ Yes, this is not a Business Associate. Proceed with normal contract procedures.