

[The District is a Hybrid Covered Entity and complies with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Generally, HIPAA applies to health plans, providers, and third party intermediaries. The District has identified covered healthcare components among its agencies which are required to comply with HIPAA. The Health Information Technology for Economic and Clinical Health Act of 2009 makes HIPAA applicable to, as well as establishes direct liability for, vendors and subcontractors who meet the definition of a “Business Associate” as defined in 45 C.F.R. §164.103. This HIPAA Business Associate Compliance clause must be included in contracts which involve access to the District’s HIPAA protected data (protected health information) or creation of the same.

The HIPAA Business Associate Compliance clause is to be used for contracts with healthcare components involving transmitting, creating, accessing, receiving or maintaining any health information for files on individuals who are served by the District. Because certain vendors conducting business with District agencies are required to comply with HIPAA and are civilly and criminally liable for their failure to do so, you must verify the procuring agency’s HIPAA covered status. The procuring agency should advise you when to use this clause. The agency must also advise how to complete the clause and adapt it as necessary with business-specific language. Delete the bracketed blue instructions language when completing the clause.

Beyond use for HIPAA covered components, this clause, in whole or applicable portion, may also be used for contracts with District agencies involving healthcare and identifiable data. This clause has been adapted for use for DCHR employee benefit contracts, such as health, dental, optical and DCHR Disability Compensation contracts for employees, and any other contractors who maintain health-related files on individuals with identifiable data. Consult the Office of Healthcare Privacy and Confidentiality (OHPC) for appropriate language and to provide notice about these arrangements. The clause should also be incorporated into purchase orders, Memoranda of Agreement and Memoranda of Understanding where an agency: 1. complies with the best practices of HIPAA; 2. facilitates access to HIPAA protected data; or 3. wishes to protect similar data.

If you determine that the HIPAA Business Associate Compliance clause should be inserted into your contract, download a copy of the HIPAA Business Associate Compliance clause from [www.ocp.in.dc.gov /Policies and Procedures Library/Templates](http://www.ocp.in.dc.gov/Policies%20and%20Procedures%20Library/Templates).

The contracting officer, in collaboration with agency program staff and OHPC, should brief potential contractors about the HIPAA requirements.]

H.X HIPAA BUSINESS ASSOCIATE COMPLIANCE

For the purpose of this agreement [AGENCY], a covered component within the District of Columbia’s Hybrid Entity will be referred to as a “Covered Entity” as that term is defined by the Health Insurance Portability and Accountability Act of 1996, as amended (“HIPAA”) and associated regulations promulgated at 45 CFR Parts 160, 162 and 164 as amended (“HIPAA Regulations”) and [INSERT VENDOR NAME], as a recipient of Protected Health Information or electronic Protected Health Information from [AGENCY], is a “Business Associate” as that term is defined by HIPAA.

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the HIPAA Regulations.

1. Definitions

- a. **Business Associate** means a person or entity, who, on behalf of the District government or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of the District or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity for the District, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in 45 CFR § 164.501), management, administrative, accreditation, or financial services to or for the District, or to or for an organized health care arrangement in which the District participates, where the provision of the service involves the disclosure of protected health information from the District or arrangement, or from another business associate of the District or arrangement, to the person. A covered entity may be a business associate of another covered entity.

A Business Associate includes, (i) a Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information; (ii) a person that offers a personal health record to one or more individuals on behalf of the District; (iii) a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

A *Business Associate* does not include: (i) a health care provider, with respect to disclosures by a covered entity to the health care provider 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 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; (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 protected health information for such purposes, to the extent such activities are authorized by law; iv) a covered entity participating in an organized health care arrangement that performs a function, activity or service included in the definition of a Business Associate above for or on behalf of such organized health care arrangement.

- b. **Covered Entity** means 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 45 C.F.R. Parts 160 and 164 of HIPAA. With respect to this HIPAA Compliance Clause, *Covered Entity* shall also include the designated health care components of the District government's hybrid entity or a District agency following HIPAA best practices.
- c. **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.

- d. **Designated Record Set** means a group of records maintained by or for the Covered Entity that are:
 - i. The medical records and billing records about individuals maintained by or for a covered health care provider;
 - ii. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
 - iii. Records used, in whole or in part, by or for the Covered Entity to make decisions about individuals.
- e. **Health Care** means care services, or services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:
 - i. Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
 - ii. Sale or dispensing of a drug, device, equipment, or other item in accordance with the prescription.
- f. **Health Care Components** means a component or a combination of components of a hybrid entity designated by a hybrid entity. *Health Care Components* must include non-covered functions that provide services to the covered functions for the purpose of facilitating the sharing of Protected Health Information with such functions of the hybrid entity without business associate agreements or individual authorizations.
- g. **Health Care Operations** shall have the same meaning as the term “health care operations” in 45 C.F.R. § 164.501.
- h. **Hybrid Entity** means a single legal entity that is a covered entity and whose business activities include both covered and non-covered functions, and that designates health care components in accordance with 45 C.F.R. § 164.105(a)(2)(iii)(C). A *Hybrid Entity* is required to designate as a health care component, any other components of the entity that provide services to the covered functions for the purpose of facilitating the sharing of Protected Health Information with such functions of the hybrid entity without business associate agreements or individual authorizations. The District of Columbia is a Hybrid Covered Entity. Hybrid Entities are required to designate and include functions, services and activities within its own organization, which would meet the definition of Business Associate and irrespective of whether performed by employees of the Hybrid Entity, as part of its health care components for compliance with the Security Rule and privacy requirements under this Clause.
- i. **Record** shall mean any item, collection, or grouping of information that includes Protected Health Information and is maintained, collected, used, or disseminated by or for the Covered Entity.
- j. **Individual** shall have the same meaning as the term "individual" in 45 C.F.R. § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).
- k. **Individually Identifiable Health Information** is information that is health information, including demographic information collected from an individual, and;

- i. Is created or received by a health care provider, health plan, employer, or health care clearinghouse;
 - ii. Relates to the past, present, or future physical or mental health or condition of an individual; or the past, present, or future payment for the provision of health care to an individual; and
 - iii. That identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
- l. **National Provider Identifier (NPI) Rule.** "National Provider Identifier" shall mean the Standard Unique Health Identifier for Healthcare Providers; Final Rule at 45 C.F.R. Part 162.
- m. **Privacy and Security Official.** The person or persons designated by the District of Columbia, a *Hybrid Entity*, who is/are responsible for developing, maintaining, implementing and enforcing the District-wide Privacy Policies and Procedures, and for overseeing full compliance with the Privacy and Security Rules, and other applicable federal and state privacy law.
- n. **Privacy Officer.** "Privacy Officer" shall mean the person designated by the District's Privacy and Security Official or one of the District's covered components within its Hybrid Entity, who is responsible for overseeing compliance with the Covered Agency's Privacy Policies and Procedures, the HIPAA Privacy Regulations, HIPAA Security Regulations and other applicable federal and state privacy law(s). Also referred to as the agency Privacy Officer, the individual shall follow the guidance of the District's Privacy and Security Official, and shall be responsive to and report to the District's Privacy and Security Official on matters pertaining to HIPAA compliance.
- o. **Privacy Rule.** "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. part 160 and part 164, subparts A and E.
- p. **Protected Health Information.** "Protected Health Information" (PHI) or "Electronic Protected Health Information" (ePHI) means individually identifiable health information that is created or received by the Business Associate from or on behalf of the Covered Entity, or agency following HIPAA best practices, which is:
 - i. Transmitted by, created or maintained in electronic media; or
 - ii. Transmitted or maintained in any other form or medium.

PHI does not include information in the records listed in subsection (2) of the definition in 45 C.F.R. §160.103.Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.103.
- q. **Secretary.** "Secretary" shall mean the Secretary of the United States Department of Health and Human Services or his or her designee.
- r. **Security Officer.** The person designated by the Security Official or one of the District of Columbia's designated health care components, who is responsible for overseeing compliance with the Covered Agency's Privacy Policies and Procedures, the Security Rules, and other applicable federal and state privacy law(s). The Covered Agency's security officer shall follow the guidance of the District's Security Official, as well as the Associate Security Official within the Office of the Chief Technology Officer, and shall be responsive to the same on matters pertaining to HIPAA compliance.

- s. **Security Rule.** "Security Rule" shall mean the Standards for Security of Individually Identifiable Health Information at 45 C.F.R. part 164.
- t. **Workforce.** "Workforce" shall mean employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such entity, whether or not they are paid by the covered entity or business associate.

2. Obligations and Activities of Business Associate

- a. The Business Associate agrees not to use or disclose PHI or ePHI (hereinafter "PHI" or Protected Health Information") other than as permitted or required by this HIPAA Compliance Clause or as required by law.
- b. The Business Associate agrees to use appropriate safeguards and comply with administrative, physical, and technical safeguards requirements in 45 C.F.R. §§ 164.308, 164.310, 164.312 and 164.316 as required by § 13401 of the Health Information Technology Economic and Clinical HealthACT (February 18, 2010) ("HITECH"), to maintain the security of the PHI and to prevent use or disclosure of such PHI other than as provided for by this Clause. Business Associate acknowledges that, pursuant to HITECH, it must comply with the Security Rule and privacy provisions detailed in this Clause. As such, Business Associate is under the jurisdiction of the United States Department of Health and Human Services and is directly liable for its own compliance. A summary of HIPAA Security Rule standards, found at Appendix A to Subpart C of 45 C.F.R. § 164 is as follows:

Administrative Safeguards

Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement (R)

Physical Safeguards

Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A)
--------------------------	---------------	----------------------------------------------------------------------------------------------------------

		Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)

Technical Safeguards (see § 164.312)

Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

- c. The Business Associate agrees to name a Privacy and/or Security Officer who is accountable for developing, maintaining, implementing, overseeing the compliance of and enforcing compliance with this Clause, the Security Rule and other applicable federal and state privacy law within the Business Associate's business. The Business associate reports violations and conditions to the District-wide Privacy and Security Official and/or the Agency Privacy Officer of the covered component within the District's Hybrid Entity.
- d. The Business Associate agrees to establish procedures for mitigating, and to mitigate to the extent practicable, any deleterious effects that are known to the Business Associate of a use or disclosure of PHI by the Business Associate in violation of the requirements of this Clause.
- e. The Business Associate agrees to report to Covered Entity, in writing, any use or disclosure of the PHI not permitted or required by this HIPAA Compliance Clause or other incident or condition arising out the Security Rule, including breaches of unsecured PHI as required at 45 CFR §164.410, to the District-wide Privacy and Security Official or agency Privacy Officer within ten (10) days from the time the Business Associate becomes aware of such unauthorized use or disclosure. However, if the Business Associate is an agent of the District (i.e., performing delegated essential governmental functions), the Business Associate must report the incident or condition immediately. Upon the determination of an actual data breach, and in consultation with the District's Privacy and Security Official, the Business Associate will handle breach notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media, on behalf of the District.
- f. The Business Associate agrees to ensure that any workforce member or any agent, including a subcontractor, agrees to the same restrictions and conditions that apply through this Clause with respect to PHI received from the Business Associate, PHI created by the Business Associate, or PHI received by the Business Associate on behalf of the Covered Entity.
- g. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate

agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information

- h. Initially, within ten (10) days following the commencement of this Contract, or within ten (10) days of a new or updated agreement with a subcontractor, the Business Associate agrees to provide the District a list of all subcontractors who meet the definition of a Business Associate. Additionally, Business Associate agrees to ensure its subcontractors understanding of liability and monitor, where applicable, compliance with the Security Rule and applicable privacy provisions in this Clause.
- i. The Business Associate agrees to provide access within five business days, at the request of the Covered Entity or an Individual, at a mutually agreed upon location, during normal business hours, and in a format as directed by the District Privacy Official or agency Privacy Officer, or as otherwise mandated by the Privacy Rule or applicable District of Columbia laws, rules and regulations, to PHI in a Designated Record Set, to the Covered Entity or an Individual, to facilitate the District's compliance with the requirements under 45 C.F.R. §164.524.
- j. The Business Associate agrees to make any amendment(s) within five business days to the PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR 164.526 in a format **[agency should insert appropriate terms for amendment if applicable or]** as directed by the District Privacy Official or agency Privacy Officer in order to facilitate the District's compliance with the requirements under 45 C.F.R. §164.526.
- k. The Business Associate agrees to use the standard practices of the Covered Entity to verify the identification and authority of an Individual who requests the PHI in a Designated Record Set of a recipient of services from or through the Covered Entity. The Business Associate agrees to comply with the applicable portions of the Identity And Procedure Verification Policy **[attach Policy]**, attached hereto as Exhibit A and incorporated by reference.
- l. The Business Associate agrees to record authorizations and log such disclosures of PHI and information related to such disclosures as would be required for the Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528 and applicable District of Columbia laws, rules and regulations.
- m. The Business Associate agrees to provide to the Covered Entity or an Individual, within five (5) business days of a request **at a mutually agreed upon location, during normal business hours, and in a format designated** **[delete bolded verbiage and insert agency appropriate terms if applicable]** by the District's Privacy and Security Official or agency Privacy Officer and the duly authorized Business Associate workforce member, information collected in accordance with Paragraph (i) of this Section above, to permit the Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528, and applicable District of Columbia laws, rules and regulations.
- n. The Business Associate agrees to make internal practices, books, and records, including policies and procedures, and PHI, relating to the use and disclosure of PHI received from the Business Associate, or created, or received by the Business Associate on behalf of the Covered Entity, available to the Covered Entity, or to the Secretary, within five (5) business days of their request and **at a mutually agreed upon location, during normal business hours, and in a format designated** **[delete bolded verbiage and insert negotiated terms if applicable]** by the District Privacy and Security Official or agency Privacy Officer and the duly authorized Business

Associate workforce member, or in a time and manner designated by the Secretary, for purposes of the Secretary in determining compliance of the Covered Entity with the Privacy Rule.

- o. To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, the Business Associate agrees to comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s).
- p. As deemed necessary by the District, the Business Associate agrees to the monitoring and auditing of items listed in paragraph 2 of this Clause, as well as data systems storing or transmitting PHI, to verify compliance.
- q. The Business Associate may aggregate PHI in its possession with the PHI of other Covered Entities that Business Associate has in its possession through its capacity as a Business Associate to other Covered Entities provided that the purpose of the aggregation is to provide the Covered Entity with data analyses to the Health Care Operations of the Covered Entity. Under no circumstances may the Business Associate disclose PHI of one Covered Entity to another Covered Entity absent the explicit written authorization and consent of the Privacy Officer or a duly authorized workforce member of the Covered Entity.
- r. Business Associate may de-identify any and all PHI provided that the de-identification conforms to the requirements of 45 C.F.R. § 164.514(b) and any associated HHS guidance. Pursuant to 45 C.F.R. § 164.502(d)(2), de-identified information does not constitute PHI and is not subject to the terms of this HIPAA Compliance Clause.

3. Permitted Uses and Disclosures by the Business Associate

- a. Except as otherwise limited in this HIPAA Compliance Clause, the Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, the Covered Entity as specified in the Contract, provided that such use or disclosure would not violate Subpart E of 45 CFR § 164 if the same activity were performed by the Covered Entity or would not violate the minimum necessary policies and procedures of the Covered Entity.
- b. Except as otherwise limited in this HIPAA Compliance Clause, the Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
- c. Except as otherwise limited in this HIPAA Compliance Clause, the Business Associate may disclose PHI for the proper management and administration of the Business Associate, provided that the disclosures are required by law, or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential 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 Business Associate of any instances of which it has knowledge that the confidentiality of the information has been breached.
- d. Except as otherwise limited in this HIPAA Compliance Clause, the Business Associate may use PHI to provide Data Aggregation services to the Covered Entity as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).
- e. Business Associate may use PHI to report violations of the Law to the appropriate federal and District of Columbia authorities, consistent with 45 C.F.R. § 164.502(j)(1).

4. Additional Obligations of the Business Associate

- a. Business Associate shall submit a written report to the Covered Entity that identifies the files and reports that constitute the Designated Record Set of the Covered Entity. Business Associate shall submit said written report to the Privacy Officer no later than thirty (30) days after the commencement of the HIPAA Compliance Clause. In the event that Business Associate utilizes new files or reports which constitute the Designated Record Set, Business Associate shall notify the Covered Entity of said event within thirty (30) days of the commencement of the file's or report's usage. The Designated Record Set file shall include, but not be limited to the identity of the following:
- i. Name of the Business Associate of the Covered Entity;
 - ii. Title of the Report/File;
 - iii. Confirmation that the Report/File contains Protected Health Information (Yes or No);
 - iv. Description of the basic content of the Report/File;
 - v. Format of the Report/File (Electronic or Paper);
 - vi. Physical location of Report/File;
 - vii. Name and telephone number of current member(s) of the workforce of the Covered Entity or other District of Columbia government agency responsible for receiving and processing requests for Protected Health Information; and
 - viii. Supporting documents if the recipient/personal representative has access to the Report/File.
- b. Business Associate must provide assurances to the Covered Entity that it will continue to employ sufficient administrative, technical and physical safeguards, as described under the Security Rule, to protect and secure the Covered Entity's ePHI entrusted to it. These safeguards include:
- i. The Business Associate agrees to administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that the Business Associate creates, receives, maintains or transmits on behalf of the covered entity.
 - ii. The Business Associate agrees to report to the Covered Entity any security incident of which it becomes aware, including any attempts to access ePHI, whether those attempts were successful or not.
 - iii. This Business Associate Agreement may be terminated if the Covered Entity determines that the Business Associate has materially breached the agreement.
 - iv. The Business Associate agrees to make all policies and procedures, and documents relating to security, available to the Secretary of HHS for the purposes of determining the covered entity's compliance with HIPAA.
 - v. This agreement continues in force for as long as the Business Associate retains any access to the Covered Entity's ePHI.
 - vi. With respect to the subset of PHI known as ePHI as defined by HIPAA Security Standards at 45 C.F.R. Parts 160 and 164, subparts A and C (the "Security Rule"), if in performing the Services, Business Associate, its employees, agents, subcontractors and

any other individual permitted by Business Associate will have access to any computer system, network, file, data or software owned by or licensed to Provider that contains ePHI, or if Business Associate otherwise creates, maintains, or transmits ePHI on Provider's behalf, Business Associate shall take reasonable security measures necessary to protect the security of all such computer systems, networks, files, data and software. With respect to the security of ePHI, Business Associate shall: (A) Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the Provider; (B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; and (C) Report to the Provider any security incident of which it becomes aware.

- vii. Business Associate agrees not to electronically transmit or permit access to PHI unless such transmission or access is authorized by this Addendum and the Agreement and further agrees that it shall only transmit or permit such access if such information is secured in a manner that is consistent with applicable law, including the Security Rule. For purposes of this Addendum, "encrypted" shall mean the reversible conversion of readable information into unreadable, protected form so that only a recipient who has the appropriate "key" can convert the information back into original readable form. If the Covered Entity stores, uses or maintains PHI in encrypted form, or in any other secured form acceptable under the security regulations, Covered Entity shall promptly, at request, provide with the key or keys to decrypt such information and will otherwise assure that such PHI is accessible by upon reasonable request.
- viii. In the event Business Associate performs functions or activities involving the use or disclosure of PHI on behalf of Covered Entity that involve the installation or maintenance of any software (as it functions alone or in combination with any hardware or other software), Business Associate shall ensure that all such software complies with all applicable standards and specifications required by the HIPAA Regulations and shall inform of any software standards or specifications not compliant with the HIPAA Regulations.
- c. At the request of the Covered Entity, the Business Associate agrees to amend this agreement to comply with all HIPAA mandates.

5. Sanctions

Business Associate agrees that its workforce members, agents and subcontractors who violate the provisions of HIPAA or other applicable federal or state privacy law will be subject to discipline in accordance with Business Associate's Personnel Policy and applicable collective bargaining agreements. Business Associate agrees to impose sanctions consistent with Business Associate's personnel policies and procedures and applicable collective bargaining agreements with respect to persons employed by it. Members of the Business Associate Workforce who are not employed by Business Associate are subject to the policies and applicable sanctions for violation of this Compliance Clause as set forth in business associate agreements. In the event Business Associate imposes sanctions against any member of its workforce, agents and subcontractors for violation of the provisions of HIPAA or other applicable federal or state privacy laws, the Business Associate shall inform the District Privacy Official or the agency Privacy Officer of the imposition of sanctions.

6. Obligations of the Covered Entity

- a. The Covered Entity shall notify the Business Associate of any limitation(s) in its Notice of Privacy Practices of the Covered Entity in accordance with 45 C.F.R. § 164.520, to the extent that such limitation may affect the use or disclosure of PHI by the Business Associate.
- b. The Covered Entity shall notify the Business Associate of any changes in, or revocation of, permission by the Individual to the use or disclosure of PHI, to the extent that such changes may affect the use or disclosure of PHI by the Business Associate.
- c. The Covered Entity shall notify the Business Associate of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect the use or disclosure of PHI by the Business Associate.

7. Permissible Requests by Covered Entity

Covered Entity shall not request the Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule and Subpart E of 45 CFR § 164 if done by the Covered Entity.

8. Representations and Warranties.

The Business Associate represents and warrants to the Covered Entity:

- a. That it is duly organized, validly existing, and in good standing under the laws of the jurisdiction in which it is organized or licensed, it has the full power to enter into this HIPAA Compliance Clause and it, its employees, agents, subcontractors, representatives and members of its workforce are licensed and in good standing with the applicable agency, board, or governing body to perform its obligations hereunder, and that the performance by it of its obligations under this HIPAA Compliance Clause has been duly authorized by all necessary corporate or other actions and will not violate any provision of any license, corporate charter or bylaws;
- b. That it, its employees, agents, subcontractors, representatives and members of its workforce are in good standing with the District of Columbia, that it, its employees, agents, subcontractors, representatives and members of its workforce will submit a letter of good standing from the District of Columbia, and that it, its employees, agents, subcontractors, representatives and members of its workforce have not been de-barred from being employed as a contractor by the federal government or District of Columbia;
- c. That neither the execution of this HIPAA Compliance Clause, nor its performance hereunder, will directly or indirectly violate or interfere with the terms of another agreement to which it is a party, or give any governmental entity the right to suspend, terminate, or modify any of its governmental authorizations or assets required for its performance hereunder. The Business Associate represents and warrants to the Covered Entity that it will not enter into any agreement the execution or performance of which would violate or interfere with this HIPAA Compliance Clause;
- d. That it is not currently the subject of a voluntary or involuntary petition in bankruptcy, does not currently contemplate filing any such voluntary petition, and is not aware of any claim for the filing of an involuntary petition;

- e. That all of its employees, agents, subcontractors, representatives and members of its workforce, whose services may be used to fulfill obligations under this HIPAA Compliance Clause are or shall be appropriately informed of the terms of this HIPAA Compliance Clause and are under legal obligation to the Business Associate, by contract or otherwise, sufficient to enable the Business Associate to fully comply with all provisions of this HIPAA Compliance Clause. Modifications or limitations that the Covered Entity has agreed to adhere to with regards to the use and disclosure of PHI of any individual that materially affects or limits the uses and disclosures that are otherwise permitted under the Privacy Rule will be communicated to the Business Associate, in writing, and in a timely fashion;
- f. That it will reasonably cooperate with the Covered Entity in the performance of the mutual obligations under this Contract;
- g. That neither the Business Associate, nor its shareholders, members, directors, officers, agents, subcontractors, employees or members of its workforce have been excluded or served a notice of exclusion or have been served with a notice of proposed exclusion, or have committed any acts which are cause for exclusion, from participation in, or had any sanctions, or civil or criminal penalties imposed under, any federal or District healthcare program, including but not limited to Medicare or Medicaid, or have been convicted, under federal or District law (including without limitation following a plea of *nolo contendere* or participation in a first offender deferred adjudication or other arrangement whereby a judgment of conviction has been withheld), of a criminal offense related to (a) the neglect or abuse of a patient, (b) the delivery of an item or service, including the performance of management or administrative services related to the delivery of an item or service, under a federal or District healthcare program, (c) fraud, theft, embezzlement, breach of fiduciary responsibility, or other financial misconduct in connection with the delivery of a healthcare item or service or with respect to any act or omission in any program operated by or financed in whole or in part by any federal, District or local government agency, (d) the unlawful, manufacture, distribution, prescription or dispensing of a controlled substance, or (e) interference with or obstruction of any investigation into any criminal offense described in (a) through (d) above. The Business Associate further agrees to notify the Covered Entity immediately after the Business Associate becomes aware that any of the foregoing representations and warranties may be inaccurate or may become incorrect

9. Term and Termination

- a. **Term.** The requirements of this HIPAA Compliance Clause shall be effective as of the date of the contract award, and shall terminate when all of the PHI provided by the Covered Entity to the Business Associate, or created or received by the Business Associate on behalf of the Covered Entity, is confidentially destroyed or returned to the Covered Entity within five (5) business days of its request. The PHI shall be returned in a format mutually agreed upon by and between the Privacy Official and/or Privacy Officer or his or her designee and the appropriate and duly authorized workforce member of the Business Associate. If it is infeasible to return or confidentially destroy the PHI, protections shall be extended to such information, in accordance with the termination provisions in this Section and communicated to the Privacy Official or Privacy Officer or his or her designee. The requirement to return PHI to the District at the end of the contract term or if the contract is terminated applies irrespective of whether the Business Associate is also a covered entity under HIPAA. Where a business associate is also a covered entity, PHI provided by the District, or created or received by the Business Associate on behalf of the District, a duplicate of the record may be acceptable if mutually agreed.

b. **Termination for Cause.** Upon the Covered Entity's knowledge of a material breach of this HIPAA Compliance Clause by the Business Associate, the Covered Entity shall either:

- i. Provide an opportunity for the Business Associate to cure the breach or end the violation and terminate the Contract if the Business Associate does not cure the breach or end the violation within the time specified by the Covered Entity; or
- ii. Immediately terminate the Contract if the Business Associate breaches a material term of this HIPAA Compliance Clause and a cure is not possible.

If neither termination nor cure is feasible, the Covered Entity shall report the violation to the Secretary.

c. **Effect of Termination.**

- i. Except as provided in paragraph (ii) of this section, upon termination of the Contract, for any reason, the Business Associate shall return in a **mutually agreed upon format or confidentially destroy** *[delete bolded material and insert negotiated terms and conditions if applicable]* all PHI received from the Covered Entity, or created or received by the Business Associate on behalf of the Covered Entity within five (5) business days of termination. This provision shall apply to PHI that is in the possession of all subcontractors, agents or workforce members of the Business Associate. The Business Associate shall retain no copies of PHI in any form.
- ii. In the event that the Business Associate determines that returning or destroying the PHI is infeasible, the Business Associate shall provide written notification to the Covered Entity of the conditions that make the return or confidential destruction infeasible. Upon determination by the agency Privacy Officer that the return or confidential destruction of the PHI is infeasible, the Business Associate shall extend the protections of this HIPAA Compliance Clause to such PHI and limit further uses and disclosures of such PHI for so long as the Business Associate maintains such PHI. Additionally, the Business Associate shall:
 - (1) Retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
 - (2) Return to covered entity, or, if agreed to by covered entity, destroy the remaining PHI that the business associate still maintains in any form;
 - (3) Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to ePHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI;
 - (4) Not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out at *[Insert section number related to paragraphs (e) and (f) above under "Permitted Uses and Disclosures By Business Associate"]* which applied prior to termination; and
 - (5) Return to covered entity or, if agreed to by covered entity, destroy the PHI retained by Business Associate when it is no longer needed by Business

Associate for its proper management and administration or to carry out its legal responsibilities.

The obligations outlined in Section 2. Obligations and Activities of Business Associate shall survive the termination of this Contract.

10. Miscellaneous

- a. **Regulatory References.** A reference in this HIPAA Compliance Clause to a section in the Privacy Rule means the section as in effect or as amended.
- b. **Amendment.** The Parties agree to take such action as is necessary to amend this HIPAA Compliance Clause from time to time as is necessary for the Covered Entity to comply with the requirements of the Privacy Rule and HIPAA. Except for provisions required by law as defined herein, no provision hereof shall be deemed waived unless in writing and signed by duly authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any other right or remedy under this HIPAA Compliance Clause.
- c. **Survival.** The respective rights and obligations of the Business Associate under Section 9. Term and Termination of this HIPAA Compliance Clause and the sections of the Standard Contract Provisions for use with the District of Columbia Government Supply and Services Contracts covering Default and Termination for the Convenience of the District shall survive termination of the Contract.
- d. **Interpretation.** Any ambiguity in this HIPAA Compliance Clause shall be resolved to permit compliance with applicable federal and District of Columbia laws, rules and regulations, and the HIPAA Rules, and any requirements, rulings, interpretations, procedures, or other actions related thereto that are promulgated, issued or taken by or on behalf of the Secretary; provided that applicable federal and District of Columbia laws, rules and regulations shall supersede the Privacy Rule if, and to the extent that they impose additional requirements, have requirements that are more stringent than or provide greater protection of patient privacy or the security or safeguarding of PHI than those of the HIPAA Rules.

The terms of this HIPAA Compliance Clause amend and supplement the terms of the Contract, and whenever possible, all terms and conditions in this HIPAA Compliance Clause are to be harmonized. In the event of a conflict between the terms of the HIPAA Compliance Clause and the terms of the Contract, the terms of this HIPAA Compliance Clause shall control; provided, however, that this HIPAA Compliance Clause shall not supersede any other federal or District of Columbia law or regulation governing the legal relationship of the Parties, or the confidentiality of records or information, except to the extent that the Privacy Rule preempts those laws or regulations. In the event of any conflict between the provisions of the Contract (as amended by this HIPAA Compliance Clause) and the Privacy Rule, the Privacy Rule shall control.

- e. **No Third-Party Beneficiaries.** The Covered Entity and the Business Associate are the only parties to this HIPAA Compliance Clause and are the only parties entitled to enforce its terms. Except for the rights of individuals, as defined herein, to have access to and amend their PHI, and to an accounting of the uses and disclosures thereof, in accordance with Paragraphs (2)(f), (g) and (j), nothing in the HIPAA Compliance Clause gives, is intended to give, , or shall be construed to give or provide any benefit or right, whether directly, indirectly, or otherwise, to third persons.

- f. **Compliance with Applicable Law.** The Business Associate shall comply with all federal and District of Columbia laws, regulations, executive orders and ordinances, as they may be amended from time to time during the term of this HIPAA Compliance Clause and the Contract; to the extent they are applicable to this HIPAA Compliance Clause and the Contract.
- g. **Governing Law and Forum Selection.** This Contract shall be construed broadly to implement and comply with the requirements relating to the Privacy Rule, and other applicable laws and regulations. All other aspects of this Contract shall be governed under the laws of the District of Columbia. The Covered Entity and the Business Associate agree that all disputes which cannot be amicably resolved by the Covered Entity and the Business Associate regarding this HIPAA Compliance Clause shall be litigated before the District of Columbia Contract Appeals Board, the District of Columbia Court of Appeals, or the United States District Court for the District of Columbia having jurisdiction, as the case may be. The Covered Entity and the Business Associate expressly waive any and all rights to initiate litigation, arbitration, mediation, negotiations and/or similar proceedings outside the physical boundaries of the District of Columbia and expressly consent to the jurisdiction of the above tribunals.
- h. **Indemnification.** The Business Associate shall indemnify, hold harmless and defend the Covered Entity from and against any and all claims, losses, liabilities, costs, and other expenses incurred as a result or arising directly or indirectly out of or in connection with (a) any misrepresentation, breach of warranty or non-fulfillment of any undertaking of the Business Associate under this HIPAA Compliance Clause; and (b) any claims, demands, awards, judgments, actions and proceedings made by any person or organization, arising out of or in any way connected with the performance of the Business Associate under this HIPAA Compliance Clause.
- i. **Injunctive Relief.** Notwithstanding any rights or remedies under this HIPAA Compliance Clause or provided by law, the Covered Entity retains all rights to seek injunctive relief to prevent or stop the unauthorized use or disclosure of PHI by the Business Associate, its workforce, any of its subcontractors, agents, or any third party who has received PHI from the Business Associate.
- j. **Assistance in litigation or administrative proceedings.** The Business Associate shall make itself and any agents, affiliates, subsidiaries, subcontractors or its workforce assisting the Business Associate in the fulfillment of its obligations under this HIPAA Compliance Clause and the Contract, available to the Covered Entity, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against the Covered Entity, its directors, officers or employees based upon claimed violation of HIPAA, the Privacy Rule or other laws relating to security and privacy, except where the Business Associate or its agents, affiliates, subsidiaries, subcontractors or its workforce are a named adverse party.
- k. **Notices.** Any notices between the Parties or notices to be given under this HIPAA Compliance Clause shall be given in writing and delivered by personal courier delivery or overnight courier delivery, or by certified mail with return receipt requested, to the Business Associate or to the Covered Entity, to the addresses given for each Party below or to the address either Party hereafter gives to the other Party. Any notice, being addressed and mailed in the foregoing manner, shall be deemed given five (5) business days after mailing. Any notice delivered by personal courier delivery or overnight courier delivery shall be deemed given upon notice upon receipt.

If to the Business Associate, to

If to the Covered Entity, to

Attention: _____
Fax: _____

Attention: _____
Fax: _____

- l. **Headings.** Headings are for convenience only and form no part of this HIPAA Compliance Clause and shall not affect its interpretation.
- m. **Counterparts; Facsimiles.** This HIPAA Compliance Clause may be executed in any number of counterparts, each of which shall be deemed an original. Facsimile copies hereof shall be deemed to be originals.
- n. **Successors and Assigns.** The provisions of this HIPAA Compliance Clause shall be binding upon and shall inure to the benefit of the Parties hereto and their respective successors and permitted assigns, if any.
- o. **Severance.** In the event that any provision of this HIPAA Compliance Clause is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of the provisions of this HIPAA Compliance Clause will remain in full force and effect. In addition, in the event a Party believes in good faith that any provision of this HIPAA Compliance Clause fails to comply with the then-current requirements of the Privacy Rule, such party shall notify the other Party in writing, in the manner set forth in Section 10. Miscellaneous, Paragraph k. Notices. Within ten (10) business days from receipt of notice, the Parties shall address in good faith such concern and amend the terms of this HIPAA Compliance Clause, if necessary to bring it into compliance. If, after thirty (30) days, the HIPAA Compliance Clause fails to comply with the Privacy Rule, then either Party has the right to terminate this HIPAA Compliance Clause upon written notice to the other Party.
- p. **Independent Contractor.** The Business Associate will function as an independent contractor and shall not be considered an employee of the Covered Entity for any purpose. Nothing in this HIPAA Compliance Clause shall be interpreted as authorizing the Business Associate workforce, its subcontractor(s) or its agent(s) or employee(s) to act as an agent or representative for or on behalf of the Covered Entity.
- q. **Entire Agreement.** This HIPAA Compliance Clause, as may be amended from time to time pursuant to Section 10. Miscellaneous, Paragraph b. Amendment, which incorporates by reference the Contract, and specific procedures from the District of Columbia Department of Health Privacy Policy Operations Manual, constitutes the entire agreement and understanding between the Parties and supersedes all prior oral and written agreements and understandings between them with respect to applicable District of Columbia and federal laws, rules and regulations, HIPAA and the Privacy Rule, and any rules, regulations, requirements, rulings, interpretations, procedures, or other actions related thereto that are promulgated, issued or taken by or on behalf of the Secretary.

Attachment

Exhibit A - Identity and Procedure Verification