

**COMMONWEALTH OF PENNSYLVANIA
BUSINESS ASSOCIATE APPENDIX**

Health Insurance Portability and Accountability Act (HIPAA) Compliance

WHEREAS, the Pennsylvania Department of Health (Covered Entity) and the Contractor (Business Associate), intend to protect the privacy and provide for the security of certain Protected Health Information (PHI) to which Business Associate may have access in order to provide goods or services to or on behalf of Covered Entity, in accordance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, Public Law 111-5, the HIPAA Privacy Rule (Privacy Rule) modifying 45 CFR Parts 160 and 164, and the HIPAA Security Rule (Security Rule), modifying 45 CFR Parts 160, 162 and 164.

WHEREAS, Business Associate may receive PHI in any format including electronic form, from Covered Entity, or may create or obtain PHI from other parties for use on behalf of Covered Entity, which PHI must be handled, disclosed or used only in accordance with this Agreement, and the standards established by the HIPAA Rules.

NOW, THEREFORE, Covered Entity and Business Associate agree as follows:

1. **Definitions.** The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information (PHI), Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific Definitions:

- a. **“Business Associate”** shall have the same meaning as the term “business associate” at 45 CFR §160.103.
 - b. **“Covered Entity”** shall have the same meaning as the term “covered entity” at 45 CFR §160.103.
 - c. **“HIPAA Rules”** shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and 164.
2. **Changes in Law.** Business Associate agrees that it will comply with any changes in the HIPAA Rules by the compliance date established by any such changes and will provide the Covered Entity with written certification of such compliance.
 3. **Stated Purposes For Which Business Associate May Use Or Disclose PHI.** Except as otherwise limited in this Agreement, Business Associate shall be permitted to use or disclose PHI provided by or obtained by or obtained on behalf of Covered Entity to perform those functions, activities, or services for, or on behalf of, Covered Entity which are specified in this contract's Appendix A (Statement of Work), provided that such use or disclosure would not violate the HIPAA Rules if done by Covered Entity. Business Associate agrees to make uses, disclosures and requests for PHI consistent with Covered Entity's minimum policies and procedures.
 4. **Additional Purposes For Which Business Associate May Use Or Disclose Information.** Business Associate shall not use or disclose PHI provided by, or created or obtained on behalf of Covered Entity for any other purposes except as required by law. Business Associate shall not use PHI to de-identify the information in accordance with 45 CFR 164.514(a)-(c) without the Department's express written authorization(s). 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.

5. **Business Associate Obligations:**

- a. **Limits On Use And Further Disclosure Established By Appendix And Law.** Business Associate hereby agrees that the PHI provided by, or created or obtained on behalf of Covered Entity shall not be further used or disclosed other than as permitted or required by this Agreement, Appendix A or as required by law.
- b. **Appropriate Safeguards.** Business Associate shall establish and maintain appropriate safeguards to prevent any use or disclosure of PHI other than as provided for by this Agreement that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI that is created, received, maintained, or transmitted on behalf of the Covered Entity as required by Subpart C of 45 CFR Part 164. Appropriate safeguards shall include but are not limited to implementing:
 - i. administrative safeguards required by 45 CFR 164.308,
 - ii. physical safeguards as required by 45 CFR 164.310,
 - iii. technical safeguards as required by 45 CFR 164.312, and,
 - iv. policies and procedures and document requirements as required by 45 CFR 164.316.
- c. **Training and Guidance.** Business Associate shall provide annual training to relevant employees, contractors and subcontractors on how to prevent the improper use or disclosure of PHI. Business Associate shall also comply with annual guidance on the most effective and appropriate technical safeguards issued by the Secretary of Health and Human Services.
- d. **Reports Of Improper Use Or Disclosure or Breach.** Business Associate hereby agrees that it shall notify the Department's Project Officer and the Department's Legal Office within two (2) days of discovery of any use or disclosure of PHI not provided for or allowed by this Agreement, including breaches of unsecured PHI as required by 45 CFR 164.410. Such notification shall be written and shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or disclosed during the improper use or disclosure or Breach. Business Associate shall furnish Covered Entity with any other available information that Covered Entity is required to include in its notification to individuals under 45 CFR 164.404(c) at the time of Business Associate's notification to Covered Entity or promptly thereafter as such information becomes available. An improper use or disclosure or Breach shall be treated as discovered by the Business Associate on the first day on which it is known to the Business Associate (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of the Business Associate) or should reasonably have been known to the Business Associate to have occurred.

Business Associate Agrees that if any of its employees, agents, subcontractors, and representatives use or disclose PHI received from, or created or received on behalf of, Covered Entity, or any derivative de-identified information in a manner not provided for in this Agreement, Business Associate shall ensure that such employees, agents, subcontractors, and business representatives shall receive training on Business Associate's procedure for compliance with the HIPAA Rules, or shall be sanctioned or prevented from accessing any PHI Business Associate receives from, or creates or receives on behalf of Covered Entity. Continued use of PHI in a manner contrary to the terms of this Agreement shall constitute a material breach of this Agreement.

- e. **Subcontractors And Agents.** In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors and agents 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.
- f. **Reports Of Security Incidents.** Business Associate hereby agrees that it shall notify, in writing, the Department's Project Officer within two (2) days of discovery of any Security Incident at the

time of Business Associate's notification to Covered Entity or promptly thereafter as such information becomes available.

- g. **Right Of Access To PHI.** Business Associate hereby agrees to allow an individual who is the subject of PHI maintained in a designated record set, to have access to and copy that individual's PHI within ten (10) business days of receiving a written request from the Covered Entity or an authorized individual in accordance with the HIPAA Rules. Business Associate shall provide PHI in the format requested, unless it cannot readily be produced in such format, in which case it shall be provided in standard hard copy. If any individual requests from Business Associate or its agents or subcontractors access to PHI, Business Associate shall notify Covered Entity of same within five (5) business days. Business Associate shall further conform with and meet all of the requirements of 45 CFR 164.524.
- h. **Amendment And Incorporation Of Amendments.** Within five (5) business days of receiving a request from Covered Entity or from the individual for an amendment of PHI maintained in a designated record set, Business Associate shall make the PHI available to the Covered Entity and incorporate the amendment to enable Covered Entity to comply with 45 CFR 164.526. If any individual requests an amendment from Business Associate or its agents or subcontractors, Business Associate shall notify Covered Entity of same within five (5) business days.
- i. **Provide Accounting Of Disclosures.** Business Associate agrees to maintain a record of all disclosures of PHI in accordance with 45 CFR 164.528. Such records shall include, for each disclosure, the date of the disclosure, the name and address of the recipient of the PHI, a description of the PHI disclosed, the name of the individual who is the subject of the PHI disclosed, the purpose of the disclosure, and shall include disclosures made on or after the date which is six (6) years prior to the request. Business Associate shall make such record available to the individual or the Covered Entity within ten (10) business days of a request for an accounting of disclosures and in accordance with 45 CFR 164.528.
- j. **Access To Books And Records.** Business Associate hereby agrees to make its internal practices, books, and records relating to the use or disclosure of PHI received from, or created or received by Business Associate on behalf of the Covered Entity, available to the Covered Entity and the Secretary of Health and Human Services or designee for purposes of determining compliance with the HIPAA Rules.
- k. **Return Or Destruction Of PHI.** At termination of this Agreement, Business Associate hereby agrees to return or destroy all PHI provided by or obtained on behalf of Covered Entity. Business Associate agrees not to retain any copies of the PHI after termination of this Agreement. If return or destruction of the PHI is not feasible, Business Associate agrees to extend the protections of this Agreement to limit any further use or disclosure until such time as the PHI may be returned or destroyed. If Business Associate elects to destroy the PHI, it shall certify to Covered Entity that the PHI has been destroyed.
- l. **Maintenance of PHI.** Notwithstanding section 4(k) of this Appendix, Business Associate and its subcontractors or agents shall retain all PHI throughout the term of the Agreement and shall continue to maintain the information required under section 4(h) of this Appendix for a period of six (6) years after termination of the Agreement, unless Covered Entity and Business Associate agree otherwise.
- m. **Mitigation Procedures.** Business Associate agrees to establish and to provide to Covered Entity upon request, procedures for mitigating, to the maximum extent practicable, any harmful effect from the use or disclosure of PHI in a manner contrary to this Agreement or the HIPAA Rules. Business Associate further agrees to mitigate any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this Appendix or the Privacy Rule.

- n. **Sanction Procedures.** Business Associate agrees that it shall develop and implement a system of sanctions for any employee, subcontractor, or agent who violates this Appendix or the HIPAA Rules.
- o. **Application of Civil and Criminal Penalties.** All Civil and Criminal Penalties under the HIPAA Rules shall apply to Business Associate's violation of any security provision contained in the HIPAA Rules.
- p. **Breach Notification.** Business Associate shall comply with the Breach notification requirements of 45 CFR 164. In the event that Business Associate discovers a Breach, Covered Entity may elect to directly comply with Breach notification requirements or require Business Associate to comply with all Breach notification requirements of 45 CFR 164 on behalf of Covered Entity. If Covered Entity requires Business Associate to comply with Breach notification requirements, Business Associate shall provide Covered Entity with a detailed weekly, written report, starting one week following discovery of the Breach. The report shall include, at a minimum, Business Associate's progress regarding Breach notification and mitigation of the Breach. If Covered Entity elects to directly meet the requirements of 45 CFR 164, Business Associate shall be financially responsible to Covered Entity for all resulting costs and fees incurred by Covered Entity, including, but not limited to, labor, materials, or supplies. Covered Entity may at its sole option: 1) offset amounts otherwise due and payable to Business Associate under this Agreement; or 2) seek reimbursement of or direct payment to a third party of Covered Entity's costs and fees incurred under this paragraph, Business Associate shall make payment to Covered Entity (or a third party as applicable) within thirty (30) days from the date of Covered Entity's written notice to Business Associate.
- q. **Grounds For Breach.** Any non-compliance by Business Associate with this Appendix or the HIPAA Rules will automatically be considered to be a breach of the Agreement.
- r. **Termination by Commonwealth.** Business Associate authorizes termination of this Agreement by the Commonwealth if the Commonwealth determines, in its sole discretion that the Business Associate has violated a material term of this Appendix.
- s. **Failure to Perform Obligations.** In the event Business Associate including its subcontractors or agents fails to perform its obligations under this Appendix, Covered Entity may immediately discontinue providing PHI to Business Associate. Covered Entity may also, at its option, require Business Associate to submit to a plan of compliance, including monitoring by Covered Entity and reporting by Business Associate, as Covered Entity in its sole discretion determines to be necessary to maintain compliance with this Appendix and applicable law.
- t. **Privacy Practices.** The Covered Entity will provide and Business Associate shall immediately begin using and/or distributing to clients any applicable form, including but not limited to, any form used for Notice of Privacy Practices, Accounting for Disclosures, or Authorization, upon the effective date of this Agreement, or as otherwise designated by the Program or Covered Entity. The Covered Entity retains the right to change the applicable privacy practices, documents and forms. The Business Associate shall implement changes as soon as practicable, but not later than forty-five (45) days from the date of notice of the change. The version of the Covered Entity's Notice of Privacy Practices current at the time of execution of this Agreement is Attachment 1 to this Business Associate Appendix.
- u. **Indemnification.** Business Associate shall indemnify, defend and hold harmless Covered Entity from and all claims and actions, whether in law or equity, resulting from Business Associate's Breach or other violation of the HIPAA Rules. Additionally, Business Associate shall reimburse Covered Entity for any civil monetary penalties imposed on Covered Entity as a result of Business Associate's Breach or other violation of the HIPAA Rules.

6. Obligations of Covered Entity:

- a. **Provision of Notice of Privacy Practices.** Covered Entity shall provide Business Associate with the notice of privacy practices that the Covered Entity produces in accordance with 45 CFR 164.520 (Attachment 1 to this Business Associate Appendix), as well as changes to such notice.
- b. **Permissions.** Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by individual to use or disclose PHI of which Covered Entity is aware, if such changes affect Business Associate's permitted or required uses and disclosures.
- c. **Restrictions.** Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 CFR 164.522 to the extent that such restriction may affect Business Associate's use or disclosure of PHI.



**COMMONWEALTH OF PENNSYLVANIA DEPARTMENT OF HEALTH (DOH)
NOTICE OF PRIVACY PRACTICES FOR PROTECTED HEALTH INFORMATION**

What Is This Notice For?

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review carefully.

What Do We Do To Keep Your Health Information Private?

Keeping your health information private is one of our most important responsibilities. We are committed to protecting your health information and following all laws regarding the use of your health information. You have the right to discuss your concerns about how your health information is shared. The law under the Health Insurance Portability and Accountability Act (HIPAA) says:

1. We must keep your health information from others who do not need to know it.
 2. We must make this Notice available to you, and may only use and share your health information as explained in this Notice.
-

Who May Use And See My Health Information?

Commonwealth employees, such as program administrators, may use or share your health information for treatment, payment, and healthcare operations.

Treatment: We may use or share your health information for treatment. For example, we may use health information we receive from a health care provider who has seen you, to ensure that you are referred for further needed treatment.

Payment: We may use or share your health information in order to ensure that health services you have received through our programs are paid for. For example, we may exchange information about you with another government agency, or a health care provider who has provided you with health services.

Healthcare Operations: We may use and share your health information in order to manage our programs and to make sure that they serve you well. For example, we may review your health information and share it with other Commonwealth agencies that must also keep your health information private.

What If The Commonwealth Wants To Use Or Share My Health Information For Other Reasons?

You will be asked to sign a separate form, called an authorization form, allowing your health information to be used or shared other than for treatment, payment or business operations. The authorization form limits what health information may be used or sent, and says where and to whom the information may be sent. You can cancel the authorization at any time by letting us know in writing.

Your written authorization is required for the use and disclosure of:

1. Psychotherapy notes (with limited exceptions to include certain treatment, payment or healthcare operations).
 2. Marketing purposes (with limited exceptions).
 3. Disclosure in exchange for remuneration on behalf of the recipient of your protected health information.
-

What Rights Do I Have With Regard To My Health Information

You have the following rights with respect to your health information:

1. To amend your information. If you think some of your health information is incorrect or incomplete, you may ask that corrected or new information be added by making a request in writing to the HIPAA Contact Office. You must state why you think the correction or new information is necessary. We do not have to make the requested amendment. If we do, you may ask that the corrected or new information be sent to others who have received your health information from us. If we deny your request, you have the right to file a statement of disagreement with us and any future disclosures of the disputed information will include your statement.
2. To tell us that you want your health information to be sent somewhere else. We will again ask you to sign an authorization form. You may be charged for the cost of the copies and sending them. If we have HIV or substance abuse information about you, we cannot release it without a special signed, written authorization from you that complies with the laws governing HIV or substance abuse records. Certain other laws that we must comply with may require us to follow the special requirements of those laws in addition to HIPAA.
3. To inspect and copy certain health information. To inspect and copy your protected health information, you must submit your request in writing to the HIPAA Contact Office. If you request a copy of the information, we may charge a reasonable fee for the costs of copying, mailing, or other supplies associated with your request. You may not see the private notes taken by a mental health provider, health information compiled as part of a legal case, or in other limited circumstances. In some cases, if we deny your request to see your health information, you may request a review of the denial.
4. To get a list of where we shared your health information for the last 6 years, unless it was shared for treatment, payment, or healthcare operations. If you ask for more than one list a year, you may be charged for the cost of providing the list. Your request for your health information must be made in writing to the HIPAA Contact Office.
5. To request that the Department communicate with you in a certain way or at a certain location. For example, you can ask that we only contact you by mail or phone, or at an address or phone number other than at your home.
6. To request a restriction or limitation on your health information that we use or disclose for treatment, payment, or health care operations. You also can request a limit on your health information that we disclose to someone who is involved in your care such as a family member or friend. We do not have to agree to the restriction or limitations. If we do agree to the request, we will honor the restriction until you revoke it or we notify you. To request restrictions make a request to the HIPAA Contact Office, you must make your request in writing and tell us what information you want to limit.
7. To be notified in the event that we (or a Business Associate) discover a breach of unsecured protected health information.

Could My Health Information Be Used Or Released Without My Authorization?

We follow laws that tell us when we have to share health information, even if you do not sign an authorization form. We will use or release your health information:

1. For public health reasons, including to prevent or control disease or injury; or report births or deaths, suspected abuse or neglect, reactions to medications or problems with certain health-related products.
2. To prevent serious threats to your health or safety or that of another person or the public.
3. To carry out treatment, payment or healthcare operations.
4. To carry out administrative functions your information may be released to specific employees who assist in the administration of the benefits.
5. To help health oversight agencies monitor the health care system, government programs, and compliance with civil rights laws, including for audits, investigations, inspections, or licensing purposes.

6. If a court orders us to, or if we receive a subpoena and receive certain assurances from the person seeking the information.
 7. To law enforcement officials, if we receive a proper request and the request meets all other legal requirements.
 8. To coroners, medical examiners or funeral directors, in order to help identify a deceased person, determine the cause of death, or perform other legally authorized duties.
 9. To organ procurement organizations, if you are an organ donor or as legally required.
 10. For health-related research that meets applicable legal requirements.
 11. To military authorities, if you were or are a member of the armed forces and the request is made by appropriate military command authorities.
 12. To authorized federal officials for national security purposes.
 13. To Workers Compensation for work-related injuries.
 14. To other government benefit programs in order to coordinate or improve administration and management of the programs.
 15. To family or others involved in your treatment or financial affairs, if you have indicated that we can do so or if we can reasonably infer that you do not object.
 16. As otherwise required by law.
-

When Is This Notice Effective?

This Notice went into effect on May, 2013.

May I Have A Copy Of This Notice?

You have a right to a paper copy of this Notice of Privacy Practice at any time. Even if you have agreed to receive this notice electronically, you are still entitled to a paper copy. We reserve the right to change this Notice, and to apply the new practices to all of your health information, including information we received before the Notice was changed. If we change this Notice and you are still in our Program, we will send you a new one upon request. You are entitled to the most current copy of the Notice. You can find the most current notice at <https://www.health.pa.gov/hipaa>

Contact Information for Complaints or Questions

If you have questions or feel your privacy rights have been violated, you can ask questions or complain by writing to or calling the **HIPAA Contact Office, Department of Health, 8th Floor West, Health and Welfare Bldg. Harrisburg, PA 17120. Phone (717) 232-4019.**

You can also complain to the federal government, Secretary of Health and Human Services, by writing to: U.S. Department of Health & Human Services, Office for Civil Rights, 150 S. Independence Mall West - Suite 372, Philadelphia, PA. 19106-3499.

Will It Make Trouble For Me If I Complain?

Your services will not be affected by any complaint made to the Department Privacy Officer, Secretary of Health and Human Services or Office of Civil Rights.