**BUSINESS ASSOCIATE AGREEMENT**

Purpose: A business associate is someone who 1.) Performs functions on behalf of a covered entity (group health plan) or provides services for a covered entity; and 2.) Has access to PHI. Under the 2013 final regulations, the HIPAA privacy and security rules require a business associate agreement to be in place if the business associate has access to PHI.

This Agreement (“Agreement”) is effective upon execution by and between \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [*Insert name of business associate*] (“Business Associate”) and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [*Insert name of employer's group health plan, e.g. "Sample Co. Group Health Plan"]* (“Health Plan”).

Health Plan and Business Associate mutually agree to comply with the requirements of the implementing regulations at 45 Code of Federal Regulations (“C.F.R.”) Parts 160-64 for the Administrative Simplification provisions of Title II, Subtitle F of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). This Agreement shall supersede any prior business associate agreement.

### Privacy and Security of Protected Health Information.

* 1. **Permitted Uses and Disclosures.** Business Associate is permitted to use and disclose Protected Health Information that it creates or receives on Health Plan’s behalf or receives from Health Plan (or another business associate of Health Plan) and to request Protected Health Information on Health Plan’s behalf (collectively, “Health Plan’s Protected Health Information”) only:
     1. **Functions and Activities on Health Plan’s Behalf.** Except as otherwise limited in this Agreement, to perform functions, activities, or services for, or on behalf of Health Plan as such services may be specified in any underlying agreement(s), provided that such use or disclosure would not violate 45 C.F.R. Part 164, Subpart E “Privacy of Individually Identifiable Health Information” (the “Privacy Rule”) or 45 C.F.R. Part 164, Subpart C "Security Standards for the Protection of Electronic Protected Health Information" (the "Security Rule") if done by Health Plan.
     2. **Business Associate’s Operations.** For Business Associate’s proper management and administration or to carry out Business Associate’s legal responsibilities, provided that, with respect to disclosure of Health Plan’s Protected Health Information, either:
        1. The disclosure is Required by Law; or
        2. Business Associate obtains reasonable assurance from any person or entity to which Business Associate will disclose Health Plan’s Protected Health Information that the person or entity will:
           1. Hold Health Plan’s Protected Health Information in confidence and use or further disclose Health Plan’s Protected Health Information only for the purpose for which Business Associate disclosed Health Plan’s Protected Health Information to the person or entity or as Required by Law; and
           2. Promptly notify Business Associate (who will in turn notify Health Plan in accordance with Section 4(a)) of any instance of which the person or entity becomes aware in which the confidentiality of Health Plan’s Protected Health Information was Breached.
     3. **Minimum Necessary.** Business Associate will, in its performance of the functions, activities, services, and operations specified in Section 1(a), make reasonable efforts to use, to disclose, and to request only the minimum amount of Health Plan’s Protected Health Information reasonably necessary to accomplish the intended purpose of the use, disclosure or request, except that Business Associate will not be obligated to comply with this minimum necessary limitation if neither Business Associate nor Health Plan is required to limit the use, disclosure or request to the minimum necessary. Business Associate and Health Plan acknowledge that the phrase “minimum necessary” shall be interpreted in accordance with the American Recovery and Reinvestment Act and government guidance on the definition.
  2. **Prohibition on Unauthorized Use or Disclosure.** Business Associate will neither use nor disclose Health Plan’s Protected Health Information, except as permitted or required by this Agreement or in writing by Health Plan or as Required by Law. This Agreement does not authorize Business Associate to use or disclose Health Plan’s Protected Health Information in a manner that will violate the Privacy Rule or the Security Rule if done by Health Plan, except as set forth in Section 1(a)(ii).
  3. **Information Safeguards.**
     1. **Privacy of Health Plan’s Protected Health Information.** Business Associate will develop, implement, maintain, and use appropriate administrative, technical, and physical safeguards to protect the privacy of Health Plan’s Protected Health Information. The safeguards must reasonably protect Health Plan’s Protected Health Information from any intentional or unintentional use or disclosure in violation of the Privacy Rule and limit incidental uses or disclosures made pursuant to a use or disclosure otherwise permitted by this Agreement.
     2. **Security of Health Plan’s Electronic Protected Health Information**. Business Associate will develop, implement, maintain, and use administrative, technical, and physical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic Protected Health Information that Business Associate creates, receives, maintains, or transmits on Health Plan’s behalf as required by the Security Rule, 45 C.F.R. Part 164, Subpart C. Such safeguards will include, but not be limited to, Business Associate conducting periodic risk assessments with respect to Health Plan's Electronic Protected Health Information. Business Associate shall, to the extent reasonably possible, implement and follow recognized security practices consistent with H.R. 7898, enacted into law on January 5, 2021. Business Associate shall provide Health Plan with all information reasonably requested about such safeguards, including whether Business Associate follows such recognized security practices and, if so, which practice or practices.
  4. **Subcontractors and Agents.** Business Associate will require any of its subcontractors and agents, to which Business Associate is permitted by this Agreement or in writing by Health Plan to disclose Health Plan’s Protected Health Information and / or Electronic Protected Health Information, to agree to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information, including but not limited to compliance with the applicable requirements of 45 C.F.R. Parts 160, 162 and 164. Such agreement between Business Associate and the subcontractor or agent must be made in writing and must comply with the terms of this Agreement and the requirements outlined at 45 C.F.R. §§ 164.504(e) and 164.314. To the extent required by applicable law or other binding regulatory guidance, Business Associate shall not disclose Health Plan's Protected Health Information to a "tracking technology vendor" (as defined in guidance issued by the United States Department of Health and Human Services ("DHHS")) unless: (i) Business Associate has entered into an agreement with such tracking technology vendor in accordance with this Section 1(d); and (ii) such disclosure is permitted or required under the Privacy Rule and this Agreement.
  5. **Prohibition on Certain Activities.** Business Associate shall not: (i) sell Protected Health Information (within the meaning of 45 C.F.R. § 164.508); (ii) use or disclose Protected Health Information for fundraising purposes (within the meaning of 45 C.F.R.§ 164.514); (iii) use or disclose Protected Health Information for research (within the meaning of 45 C.F.R.§ 164.512); (iv) use genetic information for underwriting purposes (within the meaning of 45 C.F.R.§ 164.514); or (v) use or disclose Protected Health Information for marketing purposes (within the meaning of 45 C.F.R.§ 164.508). Business Associate shall not de-identify Health Plan's Protected Health Information except if required to perform activities on behalf of Health Plan, as specified in Section 1(a)(i) of this Agreement.
  6. **Reproductive Health Information.** Business Associate shall comply with all requirements imposed on business associates under the HIPAA Privacy Rule to Support Reproductive Health Care Privacy promulgated by DHHS, including, but not limited to, the attestation requirement under 45 C.F.R. § 164.509.
  7. **Substance Use Disorder Information.** The parties acknowledge and agree that records subject to 42 C.F.R. Part 2 ("Part 2") may be used and disclosed only as permitted under Part 2.

### Compliance with Transaction Standards. If Business Associate conducts in whole or part electronic Transactions on behalf of Health Plan for which DHHS has established Standards, Business Associate will comply, and will require any subcontractor or agent it involves with the conduct of such Transactions to comply, with each applicable requirement of the Transaction Rule, 45 C.F.R. Part 162 and any related operating rules. Business Associate shall comply with the National Provider Identifier requirements, if and to the extent applicable. Business Associate shall provide to Health Plan any documentation of compliance with the Transaction Rule which Health Plan may reasonably need, if any, pursuant to section 1104(b) of the Patient Protection and Affordable Care Act, as amended. Business Associate will not enter into, or permit its subcontractors or agents to enter into, any Trading Partner Agreement in connection with the conduct of Standard Transactions on behalf of Health Plan that:

### Changes the definition, data condition, or use of a data element or segment in a Standard Transaction;

### Adds any data element or segment to the maximum defined data set;

### Uses any code or data element that is marked “not used” in the Standard Transaction’s implementation specification or is not in the Standard Transaction’s implementation specification; or

### Changes the meaning or intent of the Standard Transaction’s implementation specification.

### Individual Rights.

* 1. **Access.** Business Associate will, within \_\_\_\_\_\_\_\_ [*Insert number less than thirty, e.g., 15*] calendar days following Health Plan’s request, make available to Health Plan or, at Health Plan’s direction, to an individual (or the individual’s personal representative) for inspection and obtaining copies Health Plan’s Protected Health Information about the individual that is in Business Associate’s custody or control, so that Health Plan may meet its access obligations under 45 C.F.R. § 164.524. Effective as of September 23, 2013 and thereafter, if the Protected Health Information is held electronically in a designated record set, then the individual shall have a right to obtain from Business Associate a copy of such information in the electronic form and format requested by the individual, if it is readily producible in such form and format. If it is not so readily producible, Business Associate will provide it in a readable electronic form and format as reasonably requested by Health Plan or, if Business Associate is dealing directly with the individual, the individual. Business Associate shall provide such a copy to Health Plan or, alternatively, to the individual directly, if such alternative choice is clearly, conspicuously and specifically made by the individual or Health Plan. In addition, if the individual's request for access directs that the Protected Health Information be transmitted directly to another person designated by the individual, Business Associate must provide the copy to the person designated by the individual, provided the individual's request: (i) is in writing; (ii) is signed by the individual; and (iii) clearly identifies the designated person and where to send the copy of Protected Health Information. If Business Associate provides such a copy to that designated person, Business Associate will promptly notify Health Plan of this fact.
  2. **Amendment.** Business Associate will, within \_\_\_\_ [*Insert number less than sixty, e.g., 30*] calendar days following notice from Health Plan, amend or permit Health Plan access to amend any portion of Health Plan’s Protected Health Information, so that Health Plan may meet its amendment obligations under 45 C.F.R. § 164.526.
  3. **Disclosure Accounting.** So that Health Plan may meet its disclosure accounting obligations under 45 C.F.R. § 164.528:
     1. **Disclosures Subject to Accounting.** Business Associate will record the information specified in Section 3(c)(iii) below (“Disclosure Information”) for each disclosure of Health Plan’s Protected Health Information, not excepted from disclosure accounting as specified in Section 3(c)(ii) below, that Business Associate makes to Health Plan or to a third party.
     2. **Disclosures Not Subject to Accounting.** Business Associate will not be obligated to record Disclosure Information or otherwise account for disclosures of Health Plan’s Protected Health Information if Health Plan need not account for such disclosures.
     3. **Disclosure Information.** With respect to any disclosure by Business Associate of Health Plan’s Protected Health Information that is not excepted from disclosure accounting by Section 3(c)(ii) above, Business Associate will record the following Disclosure Information as applicable to the type of accountable disclosure made:
        1. **Disclosure Information Generally.** Except for repetitive disclosures of Health Plan’s Protected Health Information as specified in Section 3(c)(iii)(B) below, the Disclosure Information that Business Associate must record for each accountable disclosure is (i) the disclosure date, (ii) the name and (if known) address of the entity to which Business Associate made the disclosure, (iii) a brief description of Health Plan’s Protected Health Information disclosed, and (iv) a brief statement of the purpose of the disclosure.
        2. **Disclosure Information for Multiple Disclosures.** For multiple disclosures of Health Plan’s Protected Health Information that Business Associate makes for a single purpose to the same person or entity (including Health Plan), the Disclosure Information that Business Associate must record is either the Disclosure Information specified in Section 3(c)(iii)(A) above for each accountable disclosure, or (i) the Disclosure Information specified in Section 3(c)(iii)(A) above for the first of the repetitive accountable disclosures, (ii) the frequency, periodicity, or number of the repetitive accountable disclosures, and (iii) the date of the last of the repetitive accountable disclosures.
     4. **Availability of Disclosure Information.** Business Associate will maintain the Disclosure Information for at least 6 years following the date of the accountable disclosure to which the Disclosure Information relates.

Business Associate will make the Disclosure Information available to Health Plan within \_\_\_\_\_\_\_\_ [*Insert number less than sixty, e.g., 30*] calendardays following Health Plan’s request for such Disclosure Information to comply with an individual’s request for disclosure accounting.

* 1. **Restriction Agreements and Confidential Communications.** Business Associate will comply with any agreement that Health Plan makes that either (i) restricts use or disclosure of Health Plan’s Protected Health Information pursuant to 45 C.F.R. § 164.522(a), or (ii) requires confidential communication about Health Plan’s Protected Health Information pursuant to 45 C.F.R. § 164.522(b), provided that Health Plan notifies Business Associate in writing of the restriction or confidential communication obligations that Business Associate must follow. Health Plan will promptly notify Business Associate in writing of the termination of any such restriction agreement or confidential communication requirement and, with respect to termination of any such restriction agreement, instruct Business Associate whether any of Health Plan’s Protected Health Information will remain subject to the terms of the restriction agreement.

### Breaches and Security Incidents.

* 1. **Reporting.**
     1. **Privacy or Security Breach.** Business Associate will report to Health Plan any use or disclosure of Health Plan’s Protected Health Information not permitted by this Agreement or in writing by Health Plan, along with any Breach or possible Breachof Health Plan’s Unsecured Protected Health Information. In connection with this report to Health Plan, Business Associate will prepare a written risk assessment for each Breach or possible Breach and shall provide a copy of such risk assessment to Health Plan. Business Associate will treat the Breach as being Discovered in accordance with HIPAA’s requirements. Business Associate will make the report to Health Plan’s Privacy Official not more than \_\_\_\_\_\_ [*Insert number less than 60, e.g., 15*] calendar days after Business Associate learns of such non-permitted use or disclosure. If a delay is requested by a law enforcement official in accordance with 45 C.F.R. § 164.412, Business Associate may delay notifying Health Plan for the time period specified by such regulation. Business Associate’s report will at least:
        1. Identify the nature of the Breach or other non-permitted use or disclosure, which will include a brief description of what happened, including the date of any Breach and the date of the discovery of any Breach;
        2. Identify Health Plan’s Protected Health Information that was subject to the non-permitted use or disclosure or Breach (such as whether full name, social security number, date of birth, home address, account number or other information were involved) on an individual-by-individual basis;
        3. Identify who made the non-permitted use or disclosure and who received the non-permitted disclosure;
        4. Identify what corrective or investigational action Business Associate took or will take to prevent further non-permitted uses or disclosures, to mitigate harmful effects and to protect against any further Breaches;
        5. Identify what steps the individuals who were subject to a Breach should take to protect themselves;
        6. Provide such other information, including a written report, as Health Plan may reasonably request.
     2. **Security Incidents.** Business Associate will report to Health Plan within \_\_\_\_\_\_\_\_ [*Insert number, e.g., 15*] calendar days any attempted or successful (A) unauthorized access, use, disclosure, modification, or destruction of Health Plan’s Electronic Protected Health Information or (B) interference with Business Associate’s system operations in Business Associate’s information systems, of which Business Associate becomes aware. Business Associate will make this report upon Health Plan’s request, except if any such security incident resulted in a disclosure or Breach of Health Plan’s Protected Health Information or Electronic Protected Health Information not permitted by this Agreement, Business Associate will make the report in accordance with Section 4(a)(i) above.
  2. **Termination of Agreement.**
     1. **Termination Resulting from the End of Relationship, Functions or Services**. This Agreement shall terminate in the event that the underlying relationship, functions, or services that give rise to the necessity of a Business Associate Agreement terminate for any reason.
     2. **Right to Terminate for Breach.** Health Plan may terminate Agreement if it determines, in its sole discretion, that Business Associate has breached any provision of this Agreement. Health Plan may exercise this right to terminate Agreement by providing Business Associate written notice of termination. Any such termination will be effective immediately or at such other date specified in Health Plan’s notice of termination.
     3. **Obligations on Termination.**
        1. **Return or Destruction of Health Plan’s Protected Health Information as Feasible.** Upon termination or other conclusion of Agreement, Business Associate will, if feasible, return to Health Plan or destroy all of Health Plan’s Protected Health Information in whatever form or medium, including all copies thereof and all data, compilations, and other works derived therefrom that allow identification of any individual who is a subject of Health Plan’s Protected Health Information. Business Associate will require any subcontractor or agent, to which Business Associate has disclosed Health Plan’s Protected Health Information as permitted by Section 1(e) of this Agreement, to if feasible return to Business Associate (so that Business Associate may return it to Health Plan) or destroy all of Health Plan’s Protected Health Information in whatever form or medium received from Business Associate, including all copies thereof and all data, compilations, and other works derived therefrom that allow identification of any individual who is a subject of Health Plan’s Protected Health Information, and certify on oath to Business Associate that all such information has been returned or destroyed. Business Associate will complete these obligations as promptly as possible, but not later than \_\_\_\_\_\_ [*Insert number, e.g., 30*] calendardays following the effective date of the termination or other conclusion of Agreement.
        2. **Procedure When Return or Destruction Is Not Feasible.** Business Associate will identify any of Health Plan’s Protected Health Information, including any that Business Associate has disclosed to subcontractors or agents as permitted by Section 1(e) of this Agreement, that cannot feasibly be returned to Health Plan or destroyed and explain why return or destruction is infeasible. Business Associate will limit its further use or disclosure of such information to those purposes that make return or destruction of such information infeasible. Business Associate will require such subcontractor or agent to limit its further use or disclosure of Health Plan’s Protected Health Information that such subcontractor or agent cannot feasibly return or destroy to those purposes that make the return or destruction of such information infeasible. Business Associate will complete these obligations as promptly as possible, but not later than \_\_\_\_\_ [*Insert number, e.g., 30*] calendar days following the effective date of the termination or other conclusion of Agreement.
        3. **Continuing Privacy and Security Obligation.** Business Associate’s obligation to protect the privacy and safeguard the security of Health Plan’s Protected Health Information as specified in this Agreement will be continuous and survive termination or other conclusion of this Agreement.

### General Provisions.

* 1. **Inspection of Internal Practices, Books, and Records.** Business Associate will make its internal practices, books, and records relating to its use and disclosure of Health Plan’s Protected Health Information available to Health Plan and to DHHS to determine Health Plan’s compliance with the Privacy Rule, 45 C.F.R. Part 164, Subpart E.
  2. **Definitions.** All terms that are used but not otherwise defined in this Agreement shall have the meaning specified under HIPAA, including its statute, regulations and other official government guidance. For purposes of this Agreement, Health Plan’s Protected Health Information encompasses Health Plan’s Electronic Protected Health Information.
  3. **Amendment to Agreement.** Upon the compliance date of any final regulation or amendment to final regulation promulgated by DHHS that affects Business Associate’s use or disclosure of Health Plan’s Protected Health Information or Standard Transactions this Agreement will automatically amend such that the obligations imposed on Business Associate remain in compliance with the final regulation or amendment to final regulation.
  4. **No Third Party Beneficiaries.** Nothing in this Agreement shall be construed as creating any rights or benefits to any third parties.

**e) Delegation to Business Associate**. To the extent the parties agree that Business Associate will carry out directly one or more of Health Plan's obligations under the Privacy Rule, Business Associate will comply with the requirements of the Privacy Rule that apply to Health Plan in the performance of such obligations**.**

**f) No Agency Relationship**. Both parties agree that Business Associate is not, and shall not be deemed to be, an agent of Health Plan.

**IN WITNESS WHEREOF,** Health Plan and Business Associate execute this Agreement in multiple originals to be effective \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [*Insert effective date, e.g., December 1, 2024*].

|  |  |
| --- | --- |
| **[*Insert name of Business Associate*]** | **[*Insert name of Health Plan*]** |
| By: | By: |
| Its: | Its: |
| Date: | Date: |

## Business Associate Agreement Checklist

|  |
| --- |
| Purpose: The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") was amended in 2009 by the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). HIPAA and the HITECH Act require that a "covered entity" enter into a business associate agreement ("BAA") with a business associate. This Checklist discusses which terms must be included in a BAA. This Checklist also discusses some optional terms which covered entities and business associates may want to consider. |

| **Mandatory Terms** | **Check if Included / Comments** |
| --- | --- |
| **1. Permitted Uses.** The BAA must establish the permitted and required uses and disclosures of protected health information ("PHI") by the business associate. | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **2. Use of PHI by Business Associate.** The BAA may not authorize the business associate to use or further disclose PHI in a manner that would violate the requirements of the Privacy Rule, if done by the covered entity. However, the BAA may permit:   1. The business associate to use or disclose PHI for the business associate’s proper management and administration (in limited circumstances); and 2. The business associate to perform data aggregation services relating to a covered entity's health care operation.   In addition, the BAA may allow the business associate to disclose such PHI if:   1. the disclosure is required by law; or 2. **(i)** the business associate obtains reasonable assurance from any person or entity to which the business associate will disclose the PHI that the person or entity will hold the PHI in confidence and use or further disclose PHI only for the purpose for which the business associate disclosed the PHI or as required by law; and   **(ii)** the person notifies the business associate of any instances of which it is aware in which the confidentiality of the PHI has been breached. | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **3. Follow BAA and HIPAA.** The business associate will not use or further disclose the information other than as permitted or required by the BAA or as required by law. | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **4. Safeguards of PHI.** The business associate must use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by the BAA. | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **5. Comply with HIPAA Security.** The business associate must comply with the applicable requirements of the Security Rule, 45 CFR Part 164, Subpart C, including using appropriate safeguards for electronic PHI ("ePHI"). | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **6. Reporting Improper Use or Disclosure.** The business associate must report to the covered entity any use or disclosure of PHI not provided for by the BAA of which it becomes aware. | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **7. Report Security Incidents.** The business associate must report to the covered entity any security incident of which it becomes aware. | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **8. Mitigation.** The business associate must mitigate, to the extent practicable, any harmful effect that is known to the business associate of a use or disclosure of PHI by the business associate in violation of the requirements of the BAA. | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **9. Restrictions on Subcontractors.** The business associate must ensure that any subcontractor, to whom the business associate provides PHI received from, or created or received by, the business associate on behalf of the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such information. | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **10. Safeguards of Subcontractors.** The business associate must ensure that any subcontractor, to whom the business associate provides ePHI agrees to implement reasonable and appropriate safeguards to protect such ePHI. | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **11. Access Rights.** The business associate must make available PHI in accordance with an individual’s access rights under 45 C.F.R. § 164.524 and the HITECH Act. The BAA should require that copies be available in electronic form. | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **12. Disclosure Accounting.** The business associate must make available the information required to provide an accounting of the disclosures in accordance with 45 CFR § 164.528 and the HITECH Act. | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **13. Make Records Available.** The business associate must make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by, the business associate, on behalf of the covered entity, available to the Secretary of the Department of Health and Human Services for purposes of determining the covered entity's compliance with HIPAA. | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **14. Return or Destroy PHI.** The business associate must, upon termination of the BAA, return or destroy the PHI it received pursuant to the agreement, if feasible. For PHI which Business Associate cannot feasibly return or destroy, Business Associate must promise to continue to safeguard the PHI and use or disclose it only for the reasons that make return or destruction infeasible. | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **15. Report Breach.** The business associate must report to the covered entity any breach of unsecured PHI in accordance with 45 C.F.R. Part 164 Subpart D. The business associate likely should include a copy of its risk assessment demonstrating why it was or was not a breach. | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **16. No Remuneration.** The business associate must not directly or indirectly receive remuneration in exchange for any PHI of an individual.  Note: Technically remuneration would be possible with an authorization and satisfaction of some additional terms. However, this is not detailed here as this would presumably be rare (many covered entities may not allow it, even if allowed by law). | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **17. Termination Upon Violation.** The business associate must permit the covered entity to terminate the BAA in case of material violation of a privacy or security provision of the BAA. | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **18. Standard Transactions.** The business associate must comply with the Administrative Requirements of 45 C.F.R. Part 162 when acting on behalf of the covered entity. These requirements include, but are not limited to:   * The business associate must comply with the Electronic Standard Transaction rules when the business associate conducts a Transaction described in 45 C.F.R. Part 162; * The business associate must not enter into a trading partner agreement on behalf of the covered entity that would violate 45 C.F.R. §162.915; * The business associate must comply with the National Provider Identification requirements contained in 45 C.F.R. §162.412; * The business associate must comply with all operating rules that apply to the covered entity, including but not limited to 45 C.F.R. §162.1403.   Note that these provisions may not be required to be included in the BAA if the business associate will never engage in such transactions. However, the covered entity likely cannot know with certainty whether this would always be true in the future. Thus, the terms likely should be included in the BAA. | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **19. Minimum Necessary.** The business associate must comply with the "minimum necessary" rules (including the requirement that the business associate limit the information to a "limited data set" to the extent practicable) when using, disclosing or requesting PHI, except when a specific exception applies under HIPAA or the HITECH Act. | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **20. Amendment of PHI.** The business associate must make available PHI for amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. §162.526. | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **21. Carrying Out Plan's Obligations.** To the extent the business associate will carry out a plan's obligation under the HIPAA Privacy Rules, the business associate must comply with the Privacy Rule requirements that apply to the plan. | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **22. Comply with Reproductive Health Care Regulations.** The BAA should ensure that the business associate complies with the April 2024 HIPAA regulations related to reproductive health care. | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

| **Strongly Suggested / Typically Included Provisions** | **Check if Included / Comments** |
| --- | --- |
| **1.** **Termination Due to Overall Relationship Ending. The BAA shall terminate in the event that the underlying relationship**, functions, or services that gives rise to the necessity of a BAA terminates for any reason. | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **2. Reporting of Violation.** The business associate may use PHI to report violations of law to the appropriate state and federal authorities, consistent with 45 CFR § 164.502(j)(i). | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **3. Restriction Requests.** 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 CFR § 164.522(a) and the HITECH Act. | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **4. Confidential Communication Requests.** The covered entity shall notify the business associate of any confidential communication requests which the covered entity has agreed to in accordance with 45 CFR § 164.522(b). | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **5. Who Determines Breach.** Describe which entity (the plan or business associate) will determine whether a breach occurred. |  |
| **6. Other Terms.** Non-HIPAA, "standard" contract terms such as:  \* Severability -- if one section is invalid, the rest remain  \* Section headings are for convenience only  \* Notices must be in writing  \* Waiver of one provision of the BAA does not waive other provisions  \* BAA drafted by all parties  \* Applicable law and venue  \* BAA may be executed in multiple counterparts  \* No Sending PHI or ePHI to locations outside United States  \* Business associate is not an "agent" of the plan | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |  |
| --- | --- |
| **Use Caution Regarding These Terms** | **Check if Included / Comments** |
| **1. Indemnification.** Indemnification (especially if one-sided and not mutual). | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **2. Reference to Other Documents.** Requirement to follow the other party's notice of privacy practices or policies and procedures. | 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |