Annotated Business Associate Agreement for Permanent Supportive Housing Developers

Made Possible Through the Support of CSH

Public Counsel has created the attached sample "Business Associate Agreement for Permanent Supportive Housing Developers" to assist permanent supportive housing developers that partner with federally qualified health centers, community clinics, hospitals, the Los Angeles County Department of Mental Health, and other "covered entities" to understand their responsibilities under the Health Insurance Portability and Accountability Act ("HIPAA").

HIPAA is a federal law that protects the privacy of health-related information. Specifically, HIPAA imposes regulations on the proper use and disclosure of protected health information ("PHI"). PHI is information in any form that (1) is created or received by a health care provider or health plan; (2) identifies an individual and (3) relates to the past, present, or future (a) physical or mental condition of an individual; (b) provision of health care to an individual; or (c) payment for provision of health care to an individual.

The HIPAA rules apply to both "covered entities" and "business associates." The term "covered entity" refers to, in part, health care providers that bill for service electronically. The term "business associate" refers to a person or organization that uses or discloses PHI information on behalf of a covered entity. Although most permanent supportive housing developers do not directly provide and bill for medical services, and are therefore not covered entities per se, an increasing number of developers are partnering with covered entities, such as community clinics, in order to provide tenants with necessary supportive services. Because the housing developer often accesses, uses, and discloses the PHI of its tenants as part of its partnership with a covered entity, these housing developers are considered business associates under HIPAA, and therefore are required to follow many of the rules concerning health information privacy and security. While previously business associates were only *contractually* liable for following the HIPAA rules, under recent legislation business associates are now directly responsible for following these rules, and potentially face civil and criminal penalties should the rules not be followed.

HIPAA requires covered entities to enter into a written agreement, known as a "business associate agreement," with each of its business associates. (Some covered entities take a very conservative approach under HIPAA and require all contractors to sign business associate agreements even if the contractor may not technically be a business associate under HIPAA.) Such agreements outline the permitted and required uses and disclosures of health information, obligations with regard to securing electronic health information, and requirements for reporting breaches of information. The attached business associate agreement is an example of one such agreement, and includes annotations explaining how the concepts apply in the setting of permanent supportive housing. Because in most situations, the covered entity will draft and present an agreement for the business associate to sign, the attached agreement is, on the whole, favorable to covered entities. In the footnotes are included areas where a business associate may want to request a change, although opportunities for negotiation may be limited.

The footnotes also contain information about best practices for housing developers who are business associates of covered entities. For example, while not strictly required to do so, business associates are strongly encouraged to encrypt electronic personal data in their possession in order to provide maximum protection to tenants' privacy and avoid unauthorized disclosure of such information. While a housing provider may hesitate to carry the financial or administrative costs of encryption, it may well be far less costly than the risks posed by unauthorized disclosure of PHI due to a security breach. (See footnote 30.)

Some of the provisions in the agreement contain bold bracketed text that indicates where the user is required to insert language to replace the bracketed terms. Other provisions contain italicized text that shows alternatives that may or may not be required. In such cases, the notes explain under what circumstances parties would choose to include the italicized language. When given a choice between two or more alternatives, each alternative is italicized and separated by a capitalized and underlined "OR."

Throughout the body of the agreement, references are made to the statutes and regulations comprising HIPAA. "CFR" refers to the Code of Federal Regulations. "USC" refers to the United States Code.

Public Counsel will update this resource periodically as required by changes in law.

This resource should not be construed as legal advice. Please contact an attorney for legal advice about your organization's specific situation. Some organizations may be subject to laws and regulations not specifically discussed in this resource.

…

Public Counsel's **Community Development Project** builds strong foundations for healthy, vibrant and economically stable communities through its comprehensive legal and capacity building services for nonprofits that assist low income neighborhoods in Los Angeles County.

If your organization needs legal assistance, or to access the latest version of this document, visit https://publiccounsel.org/services/nonprofits/or call (213) 385-2977, x 200.

NOTE: HIPAA does not supersede 42 CFR Part 2 (Confidentiality of Alcohol and Drug Abuse Patient Records), and it also defers to more stringent state laws. Therefore, it is important to consider all applicable statutes and regulations when implementing HIPAA. THIS BAA IS LIMITED TO HIPAA; THEREFORE, IF INFORMATION IS BEING EXCHANGED RELATED TO SUBSTANCE ABUSE, MENTAL HEALTH OR SEXUALLY TRANSMITTED DISEASES, THERE MAY BE ADDITIONAL RESTRICTIONS THAT APPLY THAT ARE NOT ADDRESSED IN THIS DOCUMENT.

This Business Associate Agreement, dated **[insert date]** ("Agreement"), is entered into by and between **[insert name of health care provider]** (the "Covered Entity")[1] and **[insert name of permanent supportive housing provider]** (the "Business Associate").[2] Covered Entity and Business Associate will sometimes be referred to in this Agreement individually as "Party" and collectively as "Parties".

[1] A "covered entity" is (1) a health plan; (2) a health care clearinghouse; or (3) a health care provider who transmits any health information in electronic form. 45 CFR § 160.103. Specifically, a health care provider (e.g., a private physician, government health department, hospital, community clinic, or federally qualified health center ("FQHC")) is a covered entity when it conducts certain administrative and financial transactions electronically, such as electronic eligibility inquiries or referral authorizations or billing for health care services provided to patients.

[2] A "business associate" is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. [More specifically, a "business associate" is a person an entity (other than a member of the workforce of a covered entity) who/that, on behalf of a covered entity, performs, or assists in the performance of: (A) a function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management and re-pricing, or (B) any other function or activity regulated by Subchapter C of Subtitle A of Title 45 of the Code of Federal Regulations, relating to security standards for the protection of electronic protected health information, notification in the case of breach of unsecured protected health information and privacy of individually identifiable health information) or, provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services to or for such covered entity, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement to the entity. 45 CFR § 160.103. A subcontractor of a business associate that creates, receives, maintains, or transmits protected health information on behalf of the business associate is also a "business associate."

HIPAA does not extend regulatory protection to all health information; rather, it governs only "protected health information" ("PHI"). Health information that is not PHI still might be protected, but not by HIPAA. Rather, those protections must be found under state law or other federal laws. PHI is defined as "individually identifiable health information" that is transmitted or maintained in any form or medium (electronic, oral or written). "Individually identifiable health information" is information that meets the definition of health information, including demographic information collected from an individual, and (A) identifies the individual; or (B) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. "Health information" means any information, whether oral or recorded in any form or medium that (i) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university or health care clearinghouse, and (ii) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or past, present or future payment for the provision of health care to an individual. 45 CFR § 160.103. Again, HIPAA covers PHI which is individually identifiable health information that is transmitted or maintained in any form or medium (electronic, oral or written).

A permanent supportive housing provider is a business associate under HIPAA when it provides a service to a covered entity and receives, uses, or discloses a client's PHI in the process. For example, a permanent supportive housing provider may receive PHI pertaining to its tenants from an FQHC with whom it has entered into a memorandum of understanding ("MOU") or other contractual arrangement. Similarly, a permanent supportive housing provider would

RECITALS

This Agreement is intended to protect the privacy and provide for the security of Protected Health Information (sometimes "PHI"), received, obtained, or created by Business Associate in compliance with the Health Insurance Portability and Accountability Act of 1996, as amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH") (these acts sometimes referred to collectively as "HIPAA"), and any current and future regulations promulgated under or amendments to HIPAA;

Choose one of the following:

[Business Associate provides services to Covered Entity pursuant to a Contract or Memorandum of Understanding, as detailed below (hereinafter referred to as "Service Agreement):

[Insert title and date of agreement between Covered Entity and housing provider]

Said Service Agreement is hereby incorporated by reference and shall be taken and considered as a part of this document][3]

OR

[Business Associate and Covered Entity have agreed that Business Associate will perform the following functions and provide the following services for or on behalf of the Covered Entity (hereinafter referred to as "Services"):

[Describe functions or services]];[4]

---

be considered a business associate if it receives confirmation that a prospective tenant has a diagnosable mental illness or a chronic condition from a government health department like the Los Angeles County Department of Mental Health. If the housing provider receives, uses, or discloses this information in the course of its service delivery, such as in creating a case management plan or making appropriate referrals, then it would be a business associate under HIPAA. A supportive housing provider also is a business associate if, for example, it agrees to receive referrals to house tenants who have a specific diagnosis (mental illness, HIV/AIDS, etc.) and must receive confirmation of that diagnosis from an FQHC or other covered entity as a part of the referral process.

[3] This option should be used if the permanent supportive housing provider has entered into an MOU or other similar agreement outlining the services it has agreed to provide to a health care provider or other covered entity. Because the business associate agreement must "[e]stablish the permitted and required uses and disclosures" of PHI by the business associate, 45 CFR § 164.504(e)(2)(i), the agreement should generally describe the services the business associate has agreed to provide. The simplest way to accomplish this is for the business associate agreement to incorporate by reference any previous contract, agreement, or MOU between the housing provider and the health care provider.

[4] This option should be used if no MOU or agreement exists between the housing provider and the health care provider/covered entity. An explanation of the services to be provided should be inserted here.

In the course of *[fulfilling Service Agreement obligations* OR *providing Services]* Business Associate may receive, obtain, or create PHI, as defined below. In accordance with HIPAA, which requires a Covered Entity to have a written memorandum with each of its Business Associates, the Parties wish to establish satisfactory assurances that Business Associate will appropriately safeguard PHI.

[For the avoidance of doubt, this Agreement applies only if and to the extent the Business Associate is a "business associate" as defined under 45 CFR 160.103 with respect to the Covered Entity, and the Business Associate does not, by signing this Agreement, concede that it is a "business associate" as defined under 45 CFR 160.103.][5]

In consideration of the mutual promises below, and other good and valuable consideration, the sufficiency of which is hereby acknowledged, the Parties agree as follows:[6]

[5] If the supportive housing provider uses, discloses, or receives any PHI in providing the services for the covered entity, then it is most likely a business associate. The HHS Office for Civil Rights provides that contractors whose services do not involve the use or disclosure of PHI and whose access to PHI is at most incidental and limited are not considered business associates under HIPAA and provide the example of janitorial services who may be exposed to PHI when emptying trash. *See* "Business Associate Frequently Asked Questions" on the HHS Office for Civil Rights (OCR) Privacy of Health Information website at http://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/index.html .

Given the types of use of PHI by a supportive housing provider, such as using PHI as part of providing a service and not just coming into contact with PHI incidentally, a supportive housing provider is likely to be a business associate. If the supportive housing provider believes, however, that it is not a business associate, but a covered entity is asking the supportive housing provider to sign a business associate agreement, then this bracketed language may be helpful. A housing provider's acknowledgment that it is a business associate when it is not one can unnecessarily expose the housing provider to substantial civil and criminal penalties under 42 USC §§ 1320d-5 and 1320d-6; yet its failure to enter a business associate agreement when one is required would violate HITECH. 42 USC §§ 17932(b) and 17934(c). This bracketed language provides that the agreement only applies if and to the extent the vendor is a business associate to a covered entity as defined in HIPAA and that the vendor does not, by signing the business associate agreement, concede that it is one.

[6] Covered entities are required to have business associate agreements in order to obtain "satisfactory assurance" that the business associate will appropriately safeguard the PHI it creates, receives, maintains, or transmits on behalf of the covered entity. *See* 45 CFR § 164.502(e)(1).

A. Definitions

1. "Business Associate" means **[insert name of permanent supportive housing provider].** It shall also have the same meaning as the term "business associate" set out in 45 CFR Section 160.103.

2. "Covered Entity" means **[insert name of health care provider].** It shall also have the same meaning as the term "covered entity" set out in 45 CFR Section 160.103.

3. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-91 and the regulations promulgated thereunder.

4. "Individual" means the person who is the subject of Protected Health Information and shall include a person who qualifies as a personal representative in accordance with 45 CFR Section 164.502(g).

5. "Protected Health Information" or "PHI" and "Electronic PHI" is any information, whether oral or recorded in any form or medium that is created or received by Business Associate, from or on behalf of Covered Entity, that identifies an individual or might reasonably be used to identify an individual and relates to: (i) the individual's past, present or future physical or mental health; (ii) the provision of health care to the individual; or (ii) the past, present or future payment for health care. Specific references to "Electronic PHI" shall refer only to PHI in electronic form.[7] PHI includes Genetic Information (as defined by HIPAA).

6. "Privacy Rule" means the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, subparts A and E, as amended by the Health

[7] All individually identifiable health information held or transmitted by a covered entity is protected by HIPAA. What is considered protected PHI under HIPAA in the hands of a business associate is limited to information it receives from the covered entity, or creates, maintains, uses, or transmits on behalf of the covered entity. *See* 42 USC § 17934(a); 45 CFR § 164.502(e)(1). As a result, health information a client/tenant shares with a case worker employed by a housing provider/business associate may not meet the technical definition of PHI protected by HIPAA and covered by this Agreement, unless a case worker collected this information from a tenant on behalf of a covered entity. Of course, if the housing provider is also a covered entity under HIPAA, then health information it receives from a client/tenant is protected PHI and subject to the HIPAA Privacy and Security Rules as defined in Paragraphs A.6 and A.7 of this Agreement.

Health information received by a housing provider which is not protected by HIPAA may nevertheless be protected by other statutes. There are other federal and state privacy laws that require permanent supportive housing providers to maintain the confidentiality of certain tenant personal information that it holds or uses — e.g., federal substance abuse confidentiality regulations. *See* 42 CFR, Part 2. Moreover, it is a good practice for housing providers to apply the privacy principles embodied in the HIPAA Privacy Rule to all health information it holds — there is no reason why health information a housing provider receives directly from a covered entity should be held to a greater standard of confidentiality than information received directly from a tenant.

Information Technology for Economic and Clinical Health Act ("HITECH") Act, enacted as Title XII, Subtitle D of the American Recovery and Reinvestment Act.[8]

7. "Security Rule" means the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 160 and Part 164, subparts A and C.[9]

8. "Use" and "Uses" mean, with respect to PHI, the sharing, employment, application, utilization, examination, or analysis of such PHI within Business Associate's internal operations.[10]

9. "Disclose" and "Disclosure" mean, with respect to PHI, the release, transfer, provision of access to, or divulging in any other manner of PHI outside Business Associate's internal operations.[11]

10. "Required by Law" has the same meaning as the term "required by law" in 45 CFR Section 164.103, meaning a mandate contained in law that compels an entity to make a use or disclosure of PHI and that is enforceable in a court of law.

[8] The HIPAA Privacy Rule establishes standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. It applies to all types of PHI, including oral, paper, and electronic. The Privacy Rule provides that a covered entity or business associate may not use or disclose PHI, except as permitted or required by the HIPAA regulations. Permitted uses and disclosures include: to the individual; for treatment, payment, or health care operations; with a valid authorization; in certain emergencies; and for limited law enforcement and public health purposes. *See, e.g.* 45 CFR §§ 164.502(a); 164.512.

[9] The HIPAA Security Rule establishes standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity (i.e., transmitted over or downloaded from the Internet or stored on a computer or portable computing device, including smart phones and PDAs, or computer media such as thumb drives, CDs, and DVDs.) The Security Rule addresses administrative, physical, and technical measures that must be taken to ensure the integrity, confidentiality, and accessibility of electronic PHI. It does not apply to PHI that is transmitted orally or by paper copy. The rule comes into play most frequently in a supportive housing context when PHI is transmitted by e-mail or text, or is accessed through a computer or smart phone.

[10] "Use" under this Agreement refers to using and sharing PHI within a business associate's organization. Under the Privacy Rule, an employee of a permanent supportive housing provider may not share personal health information about a tenant with another employee unless one of the Privacy Rule exceptions applies. For example, a case worker generally may not tell a fundraising department colleague that a tenant takes a certain medication because that would not be a permissible use (i.e., divulged for the purposes of treatment, payment, or health care operations), nor would it likely fall into one of the enumerated exceptions. *See* footnote 8 for some permitted uses and exceptions.

[11] "Disclosure" of PHI refers to disclosure of PHI to individuals or entities outside of the business associate's organization, for example, in the case of a permanent supportive housing provider, to a service partners or an outside property management company.

11. "Subcontractor" has the same meaning as the term "subcontractor" in 45 CFR 160.103, meaning a person or entity to whom Business Associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of Business Associate.

12. "Designated Record Set" has the same meaning as the term "designated record set" in 45 CFR 164.501.[12]

13. "Breach" has the same meaning as the term "breach" in 45 CFR Section 164.402.[13]

14. "Unsecured PHI" has the same meaning as the term "unsecured protected health information" in 45 CFR Section 164.402.[14]

[12] A "designated record set" is a group of records maintained by or for a covered entity that is (1) the medical records and billing records about individuals maintained by or for a health care provider; (2) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (3) used, in whole or in part, by or for a covered entity to make decisions about individuals. As will be discussed in Paragraph B.8 "Access to PHI", an individual has a right to inspect, obtain a copy, and request amendments to PHI that is maintained in a designated record set. Permanent supportive housing providers should create a policy regarding the types of records to be included in any designated record set in its custody or control, so that they can respond to requests appropriately and efficiently. For example, extra copies of the documents that comprise the designated record set should be excluded from the designated record set, and do not need to be made available to an individual.

[13] A "breach" is the acquisition, access, use, or disclosure of PHI in a manner not permitted under HIPAA which compromises the security or privacy of the PHI. 45 CFR § 164.402. An unauthorized acquisition, use, or disclosure of PHI is presumed to be a breach unless the covered entity or business associate demonstrates, through a risk assessment, that there is a low probability that the PHI has been compromised. 45 CFR § 164.402. The risk assessment must at least consider the following factors: (1) the nature and extent of the PHI involved; (2) the unauthorized person who used the PHI or to whom the disclosure was made; (3) whether the PHI was actually acquired or viewed; and (4) the extent to which the risk to PHI has been mitigated. The definition of "breach" excludes (1) any unintentional acquisition, access, or use of PHI by an employee of the business associate, if made in good faith and within the scope of authority and does not result in any further use or disclosure in violation of the Privacy Rule; (2) any inadvertent disclosure by a person who is authorized to access PHI to another person authorized to access PHI, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule; and (3) a disclosure of PHI where the business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. For example, a breach would occur if a case manager were to leave a case file with medical information on a public bus and it was read by another passenger. On the other hand, if an employee of a supportive housing provider who ordinarily does not have access to case files accidentally picked one up and briefly glanced at confidential medical information, that would not be considered a breach so long as that employee did not make further use of the information. A major innovation of the HITECH amendments to HIPAA is a change in the breach notification rules. For further discussion of the HITECH breach rule, *see* Paragraphs C.1 - C.7 of this Agreement and corresponding footnotes.

[14] "Unsecured" protected health information means PHI "that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals" through the use of a technology or methodology specified in guidance issued by the Secretary of Health and Human Services. 45 CFR § 164.402. The Secretary has released guidance stating that PHI is unusable, unreadable, or indecipherable if it has been encrypted or destroyed. Department of Health and Human Services Breach Notification Interim Final Rule, 74 Fed. Reg. at 42740-42743 (August 24, 2009). For more information on unsecured PHI and its relationship to a business associate's obligations under HITECH's breach rules, *see* Paragraph C.1 of this Agreement and corresponding footnote 30.

15. "Security Incident" has the same meaning as in 45 CFR Section 164.304, meaning the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system which contains Electronic PHI.[15]

16. "Secretary" means the Secretary of Health and Human Services or his or her designee.

B. Obligations of Business Associate[16]

1. Prohibited Uses and Disclosures. Business Associate shall not use or disclose PHI in a manner that would constitute a violation of the Privacy Rule if done by Covered Entity, except for the specific uses and disclosures set forth below in Paragraph B.3.[17]

[15] As discussed at Paragraph C.7, business associates are required to report security incidents to the covered entity. A "security incident" is any event that may compromise the security of a system (operating system, application, database, etc.), a network, or data that contains electronic PHI. An incident need not be real to qualify as a reportable security incident; even the threat of such an event can be considered an incident in many cases. Some examples of security incidents are: property theft (hardware or software), compromised passwords, lost access badge, unauthorized access (physical or logical), unauthorized disclosure of PHI (hardcopy or electronic), unauthorized use of accounts or privileges, tampering with data with malicious intent, misusing PHI, malicious code or virus, hoaxes that cause stress and waste of business resources, hacking (actual or attempted), criminal activity, identity theft, fraud, improper network activity (e.g., probes or network mapping from unknown or unauthorized sources), and denial of service attacks or attempts. Incidents can also be accidental or natural, for example: electrical power outages, hardware failures, human error, and acts of God (e.g., tornados, fire, earthquake, and hurricanes.) Given the breadth of potential Security Incidents, some covered entities and business associates negotiate a provision into the business associate agreement that acknowledges that "Unsuccessful Security Incidents" such as pings and other broadcast attacks on business associate's firewall, port scans, unsuccessful log-on attempts, denials of service, or any combination thereof will not result in the business associate having to report the security incident to the covered entity, unless the security incident results in unauthorized access, use, or disclosure of PHI.

[16] If the if the housing provider is a business associate, HITECH requires that the housing provider comply with the HIPAA Security Rule provisions directing implementation of administrative, physical and technical safeguards for electronic PHI and development and enforcement of related policies, procedures and documentation standards, including the designation of a security official. (*See* 42 USC §17931(a); 45 CFR §§164.308-312, and 164.16). If the housing provider is a business associate, it must also comply with specific provisions of the HIPAA Privacy Rule. Under HITECH, business associates may not use or disclose PHI in a manner that violates the Privacy Rule, or that is not permitted or required by the applicable business associate contract, or otherwise required by law.

[17] HIPAA regulations provide that the business associate agreement may not authorize the business associate to use or disclose PHI in a manner that would violate the Privacy Rule. 45 CFR § 164.504(e)(2)(i). Under HITECH, business associates are directly liable for impermissible uses and disclosures, whereas previously business associates were only contractually obligated. *See* 42 USC § 17934(a); 45 CFR 164.502(a). The consequence of this change is that business associates may now be held liable for civil or criminal penalties if they use or disclose PHI in any manner or for any purpose not permitted by the business associate agreement. *See* 42 USC §17934(c).

2. Permitted Uses and Disclosures. Business Associate shall not use or disclose PHI other than as permitted or required by this Agreement, in connection with *[fulfilling its obligations under the Service Agreement* OR *providing Services to the Covered Entity]*, or as Required by Law.[18] Business Associate acknowledges that, as between Business Associate and Covered Entity, all PHI shall be and remain the sole property of Covered Entity, including any and all forms thereof developed by Business Associate in the course of its fulfillment of its obligations pursuant to this Agreement.

3. Uses and Disclosures for Proper Management and Administration of Business Associate. Unless otherwise limited herein, in addition to any other uses and/or disclosures permitted or required by this Agreement or Required by Law, Business Associate may:
    a. Use PHI for the proper management and administration of the Business Associate or to fulfill any legal responsibilities of the Business Associate; and
    b. Disclose PHI for the proper management and administration of the Business Associate or to fulfill any legal responsibilities of the Business Associate, provided, however, that the Disclosure is Required by Law or Business Associate obtains reasonable assurances from the person to whom the PHI is Disclosed that (i) the PHI will be held confidentially and used or further Disclosed only as Required by Law or for the purpose for which it was Disclosed to the person; and (ii) the person to whom the PHI is Disclosed will notify Business Associate of any instances of which it becomes aware in which the confidentiality of the PHI has been breached.[19]

[18] This is a required provision in any business associate agreement. 45 CFR § 164.504(e)(2)(ii)(A). A business associate may not use or disclose PHI other than as permitted or required by the business associate agreement or required by law. *See* 42 USC § 17934(a). Therefore, this provision references the specific services the housing provider/business associate agreed to perform as outlined above in the Recitals section of this business associate agreement or in a separate MOU or agreement.

[19] The business associate agreement may include a provision that the business associate may use and disclose PHI for the proper management and administration of the business associate or to carry out a legal responsibility of a business associate, provided that additional requirements are met for disclosure. 45 CFR § 164.504(e)(2)(i)(A); (e)(4). For example, if a supportive housing provider decided to shred duplicate copies of its tenant records and a secretary were to see tenant PHI in the course of completing this task, such a use would be for the proper management and business of the business associate and would be permissible under this provision. Another example of a permissible use would be determining how many tenants in a building have a specific diagnosis as part of assessing what services are needed in a building.

4. Minimum Necessary. In any instance when Business Associate Uses, requests, or Discloses PHI, Business Associate shall limit such Use, Disclosure, or request to the minimum amount necessary to accomplish its intended purpose of the Use, Disclosure, or request *[consistent with the requirements of HIPAA and Covered Entity's minimum necessary policies and procedures* OR *subject to the requirements of HIPAA and the following minimum necessary requirements:* ***describe covered entity's minimum necessary policies and procedures].*** Business Associate will not be obligated to comply with this minimum necessary limitation with respect to:
    a. Disclosures to or requests by a health care provider for treatment;
    b. Uses or disclosures made to the individual who is the subject of the PHI;
    c. Uses or disclosures made pursuant to an authorization compliant with 45 CFR Section 164.508;
    d. Disclosures made to the Secretary required for compliance with or enforcement of HIPAA;
    e. Uses or disclosures that are required by law; and
    f. Uses or disclosures that are required for compliance with HIPAA.

   Business Associate agrees to comply with the Secretary's future guidance on what constitutes "minimum necessary."[20]

5. Mitigation. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known by Business Associate to result from a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement and/or applicable law, including HIPAA.[21]

[20] HIPAA requires covered entities and business associates to adhere to the "minimum necessary" standard for uses and disclosures. Under the standard, a covered entity or business associate may only use, disclose, or request the minimum amount of PHI to accomplish the intended purpose of the use, disclosure, or request. 45 CFR § 164.502(b). For example, if the services staff of the supportive housing provider includes a drug and alcohol treatment counselor who provides recovery support to tenants, a case manager may tell the counselor that a tenant has a history of substance abuse and would like to participate in recovery support services, but should not disclose that the tenant has, for example, a history of diabetes in his family, as that would be more than the minimum necessary. The minimum necessary standard does not apply in several circumstances, listed in Paragraphs B.4 (a)-(f) of this agreement.

In its introductory comments to the Final Rule, the Secretary of Health and Human Services explains that "a business associate agreement must limit the business associate's uses and disclosures of [PHI] to be consistent with the covered entity's minimum necessary policies and procedures." 78 FR 5599. The Secretary "leave[s] it to the discretion of the parties to determine to what extent the business associate agreement will include specific minimum necessary provisions." 78 FR 5599. Therefore, in this sample agreement, the parties may either simply state that the business associate's request, use, or disclosure must to be "consistent" with the covered entity's minimum necessary policies and procedures or describe such policies and procedures in greater detail.

[21] Business associates must mitigate, to the extent possible, any harmful effects that may result from using or disclosing PHI in a manner that is not permissible. For example, if a permanent supportive housing provider were to discover that an employee's e-mail address had been compromised and that an unauthorized person may have read e-mail messages containing PHI, the permanent supportive housing provider should immediately take steps to secure the e-mail address, such as changing the password. Additionally, indemnification is a common negotiating point between covered entities and business associates. Covered entities will often seek to have business associates indemnify the covered entity from any and all losses caused by a Breach, and to pay for the cost of mitigation. Supportive housing providers should be aware of the potential for such provisions and understand his/her organization's ability to indemnify the covered entity before agreeing to such a provision.

6. Appropriate Safeguards. Business Associate agrees to use appropriate administrative, technical and physical safeguards, consistent with the size and complexity of Business Associate's operations, to protect the confidentiality of PHI and to prevent the use or disclosure of PHI or Electronic PHI other than as permitted or required by this Agreement.[22]

7. Business Associate's Subcontractors. In accordance with 45 CFR 164.502(e)(1)(ii) and 45 CFR 164.308(b)(2), Business Associate shall obtain satisfactory assurances that any agent or Subcontractor that creates, receives, maintains, or transmits PHI, including Electronic PHI, on behalf of Business Associate will appropriately safeguard such PHI. Business Associate shall require each agent or Subcontractor that creates, receives, maintains, or transmits PHI, including Electronic PHI, on behalf of Business Associate to sign an agreement with Business Associate containing substantially the same provisions as this Agreement, in which such agent or Subcontractor agrees to the same restrictions and conditions that apply to Business Associate with respect to such PHI.[23]

---

[22] Business associates are required to use appropriate safeguards to prevent improper use and disclosure of PHI. *See* 45 CFR § 164.504(e)(2)(ii)(B). With regard to PHI that is not Electronic PHI, the specific safeguards the business associate must use are not delineated. There are, however, a series of administrative steps *covered entities* must take to protect PHI, including but not limited to designating a privacy officer; training staff; implementing administrative, technical, and physical safeguards to protect the privacy of PHI; implementing a process for individuals to make complaints; creating a sanction policy for when employees improperly use or disclose PHI; documentation and retention of HIPAA-related records and communications; mitigation of any harmful effects of improper use or disclosure; and developing and implementing written policies and procedures. *See* 45 CFR § 164.530. A housing provider may wish to follow these same administrative requirements as well in order to appropriately safeguard the PHI it possesses. Housing providers should keep in mind that safeguards are flexible, and dependent upon the size and complexity of the individual organization. *See* 45 CFR § 164.306(b)(2)(i).

With regard to documentation, HIPAA requires covered entities to retain HIPAA-related documents, including policies and procedures, records of disclosures, communications, and records of sanctions applied for six years. 45 CFR § 164.530(j). As discussed elsewhere in this agreement (Paragraphs B.8 - B.11 of this Agreement and footnotes 24-27), a business associate is required to provide the covered entity with certain information requested by the covered entity to allow the covered entity to fulfill its own HIPAA obligations — for example, a business associate must provide the covered entity information required for the covered entity to provide an accounting of PHI disclosures for six years to an individual who requests an accounting. Therefore, a business associate should also retain HIPAA-related documents, including PHI and records of disclosures, communications, policies and procedures, for at least six years. Keep in mind that other records, such as Medicaid or Section 8 records, may have longer retention periods.

The HIPAA rules do require that business associates follow specific standards for electronic PHI. Business associates are directly liable, and therefore subject to penalties, for a failure to comply with the HIPAA Security Rule — including but not limited to 45 CFR 164.308, 164.310, 164.312, and 164.316. *See* 42 USC § 17931(a). The Security Rule details a series of standards that health care providers and business associates must meet in order to meet the goals of protecting the confidentiality, accessibility, and integrity of electronic PHI. These standards are divided into three categories: administrative, physical, and technical. Administrative safeguards are policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI and to manage the conduct of the workforce in relation to electronic PHI. Physical safeguards are measures to protect electronic information systems, buildings, and equipment from hazards and unauthorized physical access. Technical safeguards refer to the use of technology to protect electronic PHI and control access to it. 45 CFR § 164.304. For example, as a part of these compliance requirements, business associates must appoint a security officer, develop written policies and procedures, document security activities, and train their workforce on how to safeguard electronic PHI.

[23] A business associate may allow a subcontractor to create, receive, maintain, or transmit PHI on its behalf only if the business associate obtains satisfactory assurances that the subcontractor will appropriately safeguard the information. 45

8. Access to PHI. Within **[insert number of days]** days of receiving a written request for access from the Covered Entity, Business Associate shall allow an Individual who is the subject of PHI maintained in a Designated Record Set in its custody or control to have access to and copy that Individual's PHI. Business Associate shall provide access to PHI to the extent and in the manner required by 45 CFR Section 164.524, and where applicable, the HITECH Act. If Business Associate maintains PHI in a Designated Record Set electronically, Business Associate must provide the PHI in electronic format if so requested. If any Individual requests directly from Business Associate or its agents or subcontractors access to PHI, Business Associate shall notify Covered Entity of same within **[insert number of days]** days,[24] and shall provide access to such PHI as directed by Covered Entity.

9. Amendment of PHI. Within **[insert number of days]** days of receiving a request from Covered Entity for an amendment of PHI maintained in a Designated Record Set, Business Associate shall provide such PHI to the Covered Entity for amendment and shall also incorporate any such amendments in the PHI maintained by Business Associate as required by 45 CFR Section 164.526. If any Individual requests an amendment of PHI from Business Associate or its agents, representatives, or subcontractors, Business

---

CFR §§ 164.502(e)(1)(ii); 164.308(b)(2). A business associate agreement must require a business associate to ensure that any such subcontractors agree to the same restrictions and conditions that apply to the business associate with respect to such PHI. 45 CFR § 164.504(e)(2)(ii)(D). Specifically, a business associate must enter into a written agreement with its subcontractors to ensure that the subcontractors are complaint with HIPAA and HITECH. 45 CFR §§ 164.314(a)(2); 164.504(e)(5). As discussed in footnote 2, the definition of "business associate" includes a subcontractor that creates, receives, maintains, or transmits PHI on behalf of the business associate. Therefore, subcontractors are directly required to comply with the HIPAA Privacy and Security rules. For example, if a business associated hires a company to handle document shredding to securely dispose of protected health information, then the shredding company would be a subcontractor, and directly liable for failure to comply with the Privacy Rule.

[24] HIPAA grants individuals a right of access to inspect and obtain a copy of PHI about that individual in a designated record set, as defined in Paragraph A.12. and footnote 12, with some exceptions, including psychotherapy notes. *See* 45 CFR § 164.524(a)(1). Business associate agreements must contain a provision are requiring the business associate to make available PHI in accordance with these rules. 45 CFR § 164.504(e)(2)(ii)(E). If the PHI is maintained electronically, the individual has the right to obtain a copy of the information in an electronic format. 42 USC § 17935(e); 45 CFR § 164.524(c)(2)(ii). Business Associates are directly liable under HITECH for a failure to provide access to a copy of electronic PHI to either the covered entity or the individual requesting it. *See* 45 CFR § 164.502(a)(4)(ii). Business associates may negotiate for a lengthier reporting time in order to ease the administrative burden of responding to multiple requests. A common time frame for a business associate to report to a covered entity an individual's information is ten business days. Business Associates can also add in language further extending the reporting time if the PHI is stored off site.

Associate shall refer such Individual to Covered Entity and notify Covered Entity of the request to amend within **[insert number of days]** days.[25] Any denial of amendment to PHI determined by Covered Entity pursuant to 45 CFR Section 164.526, and conveyed to Business Associate by Covered Entity, shall be the responsibility of Covered Entity, including resolution or reporting of all appeals and/or complaints arising from denials.

10. Accounting Rights. Within **[insert number of days]** days of notice by Covered Entity of a request for an accounting of Disclosures of PHI, Business Associate shall provide to Covered Entity an accounting of each Disclosure of PHI made by Business Associate or its employees, agents, representatives, or subcontractors, in order to permit Covered Entity to respond to a request by an Individual for an account of disclosures of PHI in accordance with HIPAA, including but not limited to 45 CFR Sections 164.528 and the applicable requirements of HITECH.[26]

---

[25] A covered entity must amend protected health information about an individual in a designated record set, including any designated record sets (or copies thereof) held by a business associate. In limited circumstances, a covered entity may deny such a request. 45 CFR § 164.526(a). Business associates must amend protected health information in such records (or copies) when requested by the covered entity. 45 CFR § 164.504(e)(2)(ii)(F).

[26] Under HIPAA, an individual has a right to receive an accounting of disclosures of PHI made by a covered entity in the six years prior to the date on which the accounting is requested. 45 CFR § 164.528(a). This right contains several exceptions, including disclosures to an individual of PHI about the individual, disclosures pursuant to an authorization, and disclosures for the purpose of carrying out treatment, payment and health care operations. *See* 45 CFR § 164.528(a)(1). However, with respect to PHI maintained in an Electronic Health Record specifically, under the more recent HITECH rules, an individual has an additional right to an accounting of disclosures of such records for treatment, payment, or healthcare operations purposes for *three years*. 42 USC § 17935(c). Business associates must make available to a covered entity the information required to provide an accounting of disclosures. 45 CFR § 164.504(e)(2)(ii)(G).

In order to provide the covered entity with the information needed, the housing provider must implement a process that allows for an accounting of PHI disclosures to be collected and maintained. Disclosure records collected and maintained by the business associate should include, at a minimum: (i) the date of disclosure; (ii) the name of the entity or person who received the PHI and, if known, the address of the entity or person; (iii) a brief description of PHI disclosed; and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the written request for a disclosure. *See* 45 CFR § 164.528(b)(2). As discussed in footnote 22, HIPAA-related documents should be retained for at least six years.

On May 31, 2011, the Secretary proposed several changes to the rules governing accounting of disclosures. First, the Secretary proposed modifying the right to an accounting by (1) limiting the provision to PHI held in a designated record set; (2) changing the accounting period from six years to three years; and (3) listing the types of disclosures that are subject to the accounting, rather than the types that are exempt. Specifically, the accounting right extends to: impermissible disclosures, disclosures for public health activities, disclosures for judicial and administrative proceedings, disclosures for law enforcement purposes, disclosures to avert a serious threat to health or safety, disclosures for military and veterans activities, and disclosures for workers' compensation. Second, the proposed regulations also create a new right to an access report detailing who has accessed an individual's electronic designated record set information for up to three years prior to the date on which the access report is requested. The access report encompasses not only disclosures, but uses of information within a covered entity's or business associate's workforce. The access report must set forth the date of access, the time of access, the person or entity who accessed the information, a description of what information was accessed if available, and a description of the action by the user if available. The Secretary has yet to issue a final rule on this matter, though a final rule is expected sometime in 2015. *See* 76 FR 31426. These provisions will need to be revisited when and if such final rules are issued.

11. Availability of Internal Practices, Books and Records to Government Agencies. Business Associate agrees to make its internal practices, books, and records relating to the Use and Disclosure of PHI available to the Secretary for purposes of determining Covered Entity's compliance with the Privacy Rule.[27]

12. Disclosures for Investigations When Requested by Secretary. Business Associate agrees to disclose PHI when requested by the Secretary to investigate or determine Business Associate's compliance with HIPAA.[28]

13. Carrying Out Obligations of Covered Entity. To the extent Business Associate carries out an obligation of Covered Entity under the Privacy Rule, Business Associate agrees to comply with the requirements of the Privacy Rule that apply to the Covered Entity in the performance of such obligation.[29]

C. Reporting of Breaches, Security Incidents, and Improper Uses or Disclosures

1. Notification to Covered Entity of Breach of Unsecured PHI. Business Associate shall notify the Covered Entity of any Breach by Business Associate, its employees, representatives, agents, or Subcontractors of Unsecured PHI that is discovered by the Business Associate.[30] Business

[27] *See* 45 CFR § 164.504(e)(2)(ii)(I).

[28] Business associates are required to disclose PHI when required by the Secretary of Health and Human Services to investigate or determine the business associate's compliance with the HIPAA Rules. 45 CFR § 164.502(a)(4)(i). Business associates face direct liability for failure to comply with this requirement. *See* 78 FR 5598-5599.

[29] This is a required provision in any business associate agreement. 45 CFR § 164.504(e)(2)(ii)(H). When a covered entity delegates a responsibility under the Privacy Rule to a business associate, the business associate would be contractually required to comply with the requirements of the Privacy Rule in the same manner as they apply to the covered entity. This likely will not be relevant in the permanent supportive housing context.

[30] HIPAA requires a business associate to report any breaches of unsecured PHI to the covered entity when the business associate discovers the breach. 45 CFR § 164.410. Recall that any acquisition, access, use, or disclosure of unsecured PHI in a manner not permitted under HIPAA is *presumed* to be a Breach unless the covered entity or business associate demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of, at a minimum, the following factors: (1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who used the PHI or to whom the disclosure was made; (3) whether the PHI was actually acquired or viewed; and (4) the extent to which the risk to the PHI has been mitigated. 45 CFR § 164.402; *see also* Paragraph A.13 of this Agreement and the corresponding footnote. HIPAA places the burden of proof on the business associate to demonstrate that the use or disclosure was not a breach; the business associate should always err on the side of notification in order to avoid any potential penalties or contractual liabilities. If, based on the risk assessment, a business associate determines that no breach has occurred, it must document its reasoning in case it or the covered entity is ever audited by the Department of Health and Human Services. *See* 45 CFR § 164.414.

Keep in mind that the obligation to notify the covered entity is limited to "unsecured PHI," which, as discussed in footnote 14 and Paragraph A.14 of this Agreement, is PHI that has not been rendered unreadable, unusable, or indecipherable through encryption or destruction of data. For this reason, the Department of Health and Human Services strongly recommends encryption of all the electronic personal data possessed by covered entities and business associates in order to provide maximum protection in the event of a security breach.

Associate shall be deemed to have discovered a Breach of Unsecured PHI if the Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the individual committing the Breach, that is an employee, officer, or other agent of the Business Associate.

2. Timeliness of Notification. Except as provided in Paragraph C.5, the notification required by Paragraph C.1 shall be made without unreasonable delay and not later than **[insert number of days]** days after the Business Associate discovers the Breach.[31]

3. Content of Notification. The notification required by Paragraph C.1 shall include, to the extent possible, all information required to provide notification to the Individual under 45 CFR Section 164.404(c), including but not limited to:[32]
   a. The identification of each Individual whose Unsecured PHI has been, or is reasonably believed by the Business Associate to have been accessed, acquired, used, or disclosed during the Breach;
   b. The date of the Breach and the date of the discovery of the Breach, if known;
   c. The scope of the Breach;
   d. A description of the types of Unsecured PHI that were involved in the Breach; and
   e. The Business Associate's response to the Breach. In the event of a Breach, Business Associate shall, in consultation with Covered Entity, mitigate, to the extent practicable, any harmful effect of such Breach known to the Business Associate.

Although HITECH does not require the business associate to notify the individuals affected by the breach, California Civil Code Section 1798.82 requires any person or business in California to report security breaches of unencrypted computerized personal data to the individuals affected. Personal data refers to a client/tenant's first name or first initial and last name, in combination with his or her social security number, driver's license or California Identification Card number, credit card information, medical information, and health insurance information. Cal. Civ. Code § 1798.82(h). Business associates should familiarize themselves with the notification requirements of the California law.

[31] HIPAA requires the notification to be made without unreasonable delay and in no case later than sixty calendar days after discovery of a breach. 45 CFR § 164.410(b). A breach is considered discovered by the business associate on the first day on which the breach is known or, through reasonable diligence, would have been known, to an employee, officer, or other agent of the business associate, other than the person committing the breach. 45 CFR 164.410(a)(2). The covered entity may wish to specify a time by which notification must be made. A business associate should negotiate with the covered entity to establish a reasonable time frame for notice.

A business associate has the burden of demonstrating proper notification to the covered entity of any and all breaches of unsecured PHI. 45 CFR § 164.414(b). Therefore, a supportive housing provider must retain accurate records of breaches and notifications.

[32] As discussed earlier, the covered entity is required to notify individuals affected by any breach of unsecured PHI. *See* 45 CFR § 164.404. In turn, HIPAA requires the business associate to provide sufficient information to the covered entity in the case of a breach to allow the covered entity to fulfill its own notification responsibilities. 45 CFR § 164.410(c).

4. Providing Information as it Becomes Available. If Business Associate is not able to provide the information specified in subparagraphs (b) through (e) of Paragraph C.3 at the time of the notification required by Paragraph C.2, Business Associate shall provide such information promptly thereafter as such information becomes available.[33]

5. Request for Delay by Law Enforcement. Business Associate may delay the notification required by Paragraph C.1 if a law enforcement official states to Business Associate that notification would impede a criminal investigation or cause damage to national security. If the law enforcement official's statement is in writing and specifies the time for which a delay is required, Business Associate shall delay notification, notice, or posting for the time period specified by the official; if the statement is made orally, Business Associate shall document the statement, including the identity of the official making the statement, and delay notification, notice, or posting temporarily and no longer than 30 days from the state of the oral statement, unless a written statement is submitted during that time.[34]

6. Notification of Improper Use or Disclosure of PHI. Business Associate agrees to report to Covered Entity any Use or Disclosure of PHI not provided for by this Agreement within **[insert number of days]** days of the date on which the Business Associate becomes aware of such use or disclosure.[35]

7. Notification of Security Incident. Business Associate agrees to report to Covered Entity any successful Security Incident within **[insert number of days]** days of the date on which the Business Associate becomes aware of such successful Security Incident.[36]

[33] *See* 45 CFR § 164.410(c)(2).

[34] *See* 45 CFR § 164.412.

[35] HIPAA and HITECH require this provision to be in all business associate agreements although the regulations do not specify a manner and time of notification. *See* 45 CFR § 164.504(e)(2)(ii)(C). Note that this obligation to notify a covered entity of unauthorized or improper use or disclosure is separate from and in addition to the breach notification requirements described in Paragraph C.1 of this Agreement and corresponding footnote which applies specifically to unsecured PHI.

[36] The HIPAA regulations require that the business associate agreement contain a provision requiring a business associate to report security incidents to the covered entity. *See* 45 CFR § 164.314(a)(2)(i)(C). The regulations do not specify a time or manner for the report. The business associate should negotiate a suitable timeframe with the covered entity.

D. Obligations of Covered Entity

1. Impermissible Use and Disclosure. Covered Entity agrees not to ask Business Associate to Use or Disclose PHI in a manner that would not be permitted under applicable federal or state laws if done by Covered Entity. Covered Entity may request Business Associate to disclose PHI directly to another party only for the purposes allowed by HIPAA and the HITECH Act.

2. Notice of Privacy Practices. Covered Entity shall provide Business Associate with the notice of privacy practices produced by Covered Entity in accordance with 45 CFR Section 164.520.[37] Covered Entity shall notify Business Associate of any limitation in any applicable notice of privacy practices in accordance with 45 CFR Section 164.520, to the extent that such limitation may affect Business Associate's Use or Disclosure of PHI.

3. Notice of Change in Permission to Use and Disclose PHI by an Individual. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by an Individual to use or disclose PHI**,** to the extent that such changes affect Business Associate's permitted or required uses.

4. Notice of Restriction in Use or Disclosure of Individual's PHI**.** Covered Entity shall notify Business Associate of any restriction to the Use or Disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR Section 164.522, to the extent that such restriction may affect Business Associate's use of PHI.[38]

E. Indemnification

1. Indemnification. Business Associate shall indemnify, defend, and hold harmless Covered Entity, including its elected and appointed officers, employees, and agents, from and against any and all liability, including but not limited to demands, claims, actions, fees, costs, penalties and fines, and expenses (including reasonable attorney and expert witness fees), arising from Business Associate's material breach of this Agreement.[39]

---

[37] A covered entity is required to provide individuals with a notice of the uses and disclosures of PHI a covered entity is permitted or required to make without an individual's written authorization. 45 CFR § 164.520(a)(1); (b)(ii).

[38] An individual has the right to request that a covered entity restrict uses or disclosures of PHI about that individual to carry out treatment, payment, or health care operations, although the covered entity is not required to agree to the requested restriction. If a covered entity does agree to the restriction, it must respect the request (except for in emergency situations). 45 CFR § 164.522(a). In order to make sure that the request is honored, the covered entity needs to inform the business associate of any restrictions that it has agreed to that may affect the business associate's operations.

[39] The covered entity may wish to include a broad indemnification clause under which the business associate agrees to pay for and defend any lawsuit, enforcement action, investigation, etc. arising out of the business associate's actions in connection with the business associate agreement. Although the business associate will likely not have enough leverage to remove this provision, the business associate may wish to request modifications to the provision, such as that the indemnification be mutual (both parties indemnify one another) or that the covered entity's own acts and omissions be excluded from the indemnification, or that the amount of the indemnity not be in excess of insurance. While HIPAA

F. Term and Termination

1. Term. This Agreement will be effective on **[insert date]** and will continue until the later of ***[insert termination date set in MOU OR date upon which Services are completed]*** and the date when all PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy the PHI, protections are extended to such information, in accordance with the provisions of Paragraph F.3 hereof.

2. Termination for Cause. In addition to and notwithstanding the term provisions set forth in this Agreement in Paragraph F.1 above, upon either Party's knowledge of a material breach of this Agreement by the other Party, the Party with knowledge of the other Party's breach shall provide the breaching Party with an opportunity to cure. Where said breach is not cured within **[insert number]** business days of the breaching Party's receipt of notice from the non-breaching Party of said breach, the non-breaching Party shall, if feasible, terminate this Agreement and **[insert MOU name or description of services**] affected by the breach. Where either Party has knowledge of a material breach by the other Party and cure is not possible, the non-breaching Party shall, if feasible, terminate this Agreement and **[insert MOU or description of services]**.[40]

3. Effect of Termination.

   [Option 1: Except as otherwise provided by this Paragraph, upon termination of this Agreement for any reason, Business Associate shall return or destroy all PHI created, received, maintained, or transmitted by Business Associate from or on behalf of the Covered Entity. This provision shall apply to PHI that is in the possession of Subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity, within **[insert number of days]** days, notification of the conditions that make return or destruction infeasible. Upon such determination, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.][41]

---

requires mitigation as outlined above, it does not require the inclusion of an indemnification provision. The Business Associate may also want to incorporate any limitation on its liability set forth in the underlying services agreement.

[40] If a covered entity or business associate is aware that the other party is in breach of the agreement, it needs to take steps to cure the breach or, if that is not possible, terminate the contract (and the MOU for services). 42 USC § 17934(b); 45 CFR §§ 164.504(e)(1)(ii); 164.314(a)(2)(i)(D). The most recent HITECH regulations removed the obligation to notify the Secretary of the Department of Health and Human Services when neither termination nor cure is feasible.

[41] The housing provider should use this option if the housing provider is to return or destroy all PHI upon termination except PHI that is determined infeasible to return or destroy.

Or

[Option 2: Upon termination of this Business Associate Agreement for any reason, Business Associate, with respect to all PHI received from covered entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:

a. Retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
b. Return to Covered Entity [or, if agreed to by Covered Entity, destroy] the remaining PHI that the Business Associate still maintains in any form;
c. Continue to use appropriate safeguards and comply with the Security Rule with respect to Electronic PHI 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;
d. 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 Paragraphs B.3.a and B.3.b above under "Uses and Disclosures for Proper Management and Administration of Business Associate" which applied prior to termination; and
e. Return to Covered Entity [or, if agreed to by Covered Entity, destroy] the PHI retained by the Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.][42]

G. Miscellaneous

1. Change in Law. The Parties agree to amend this Agreement as necessary to comply with any amendment to any provision of HIPAA, including, but not limited to, the Privacy Rule or the Security Rule, which materially alters either Party or both Parties' obligations under this Agreement.

2. Survival. The respective rights and obligations of Business Associate under Paragraph F.3 of this Agreement shall survive the termination of this Agreement.

3. Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity and Business Associate to comply with HIPAA, the Privacy Rule, and the Security Rule.

4. Notices and Communications. All instructions, notices, consents, demands, or other communications required or contemplated by this Agreement shall be in writing and shall be delivered by hand, by facsimile transmission, by overnight courier service, or by first class mail, postage prepaid, addressed to the respective Party at the appropriate facsimile number or

[42] The housing provider should use this option if the agreement authorizes the housing provider to use or disclose PHI for its own management and administration or to carry out its legal responsibilities (as this Agreement does in Paragraph B.3), and the housing provider needs to retain protected health information for such purposes after termination of the agreement. For example, if a tenant remains at the housing provider after the business associate agreement is terminated, the housing provider may need to retain the applicable PHI of the tenant.

address as set forth below, or to such other Party, facsimile number, or address as may be hereafter specified by written notice. The Parties agree to use their best efforts to immediately notify the other Party of changes in address, telephone number, and fax numbers and to promptly supplement this Business Associate Agreement as necessary with corrected information.

Covered Entity	Business Associate
[Insert name, address, phone, fax]	**[Insert name, address, phone, fax]**

5. *[Relationship to Service Agreement Provisions. In the event that a provision of this Agreement is contrary to a provision in the Service Agreement, the provision of this Agreement shall control]*.[43]

[43] Include this provision if the permanent supportive housing provider has entered into an MOU or other similar agreement outlining the services it has agreed to provide to a health care provider or other covered entity.