

SITERX PLATFORM
BUSINESS ASSOCIATE AGREEMENT

Last updated: September 26, 2021

1. **Introduction.** To the extent applicable, this Business Associate Agreement (this “**BAA**”) describes the rights and obligations of SiteRx (for purposes of this BAA, the “**Business Associate**”) and you and/or the Business, as applicable (the “**Business Entity**”), applicable to Business Associate’s provision to you of the Platform and other analytic services (for purposes of this BAA, the “**Services**”), and the terms and conditions related to the performance of such Services.

The performance of the Services may involve the Use and/or Disclosure of Protected Health Information (defined below), and the parties are entering into this BAA in furtherance of the parties’ HIPAA compliance obligations. You represent and warrant that you have the right, authority and capacity to enter into this BAA on behalf of the Business Entity and bind Business Entity hereto. This BAA is applicable only to the extent that Business Entity is a Covered Entity or business associate to a Covered Entity under HIPAA.

SUBJECT TO THE FOREGOING, BY USING THIS PLATFORM OR ANY INFORMATION PROVIDED ON THIS PLATFORM, YOU AGREE TO BE BOUND BY THIS BAA.

Please also refer to our Terms of Access at Terms of Access which are incorporated as if fully recited herein (“**Terms of Access**”). Capitalized terms that are not defined herein shall have the meaning ascribed to them in the Terms of Access.

2. **Definitions.** Capitalized terms not otherwise defined in this BAA shall have the same meaning as those terms in the Terms of Access or in the Privacy Rule and the Security Rule (defined below).
 - a) “**Breach**” when capitalized, “Breach” shall have the meaning set forth in 45 CFR § 164.402 (including all of its subsections); with respect to all other uses of the word “breach” in the Terms of Access, the word shall have its ordinary contract meaning.
 - b) “**Covered Entity**” shall have the same meaning as the term “covered entity” in 45 CFR § 160.103.
 - c) “**Electronic Protected Health Information**” or “**EPHI**” shall have the same meaning as the term “electronic protected health information” in 45 CFR § 160.103, limited to information that Business Associate creates, accesses or receives on behalf of Covered Entity.
 - d) “**HIPAA**” means collectively, the Health Insurance Portability and Accountability Act of 1996 as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009 and its implementing regulations, as amended and in effect.

- e) **“Protected Health Information”** or **“PHI”** shall have the meaning set forth in the Privacy Rule, limited to information that Business Associate creates, accesses or receives on behalf of Covered Entity. PHI includes EPHI.
- f) **“Privacy Rule”** means the Standards for Privacy of Individually Identifiable Health Information, codified at 45 CFR parts 160 and 164, Subparts A, D, and E, as currently in effect.
- g) **“Security Rule”** means the Standards for Security for the Protection of Electronic Protected Health Information, codified at 45 CFR parts 160 and 164, Subpart C.
- h) **“Unsecured Protected Health Information”** shall have the same meaning as the term “unsecured protected health information” in 45 CFR § 164.402, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

3. Business Associate Obligations.

- a) Uses and Disclosures. Business Associate shall not Use or further disclose PHI other than as permitted or required by this BAA, to perform Services or as Required By Law, provided that:
 - a.i) Such Use or Disclosure would not violate HIPAA if done by Business Entity; and
 - a.ii) Such Use or Disclosure shall be limited to the minimum necessary to accomplish the permissible purpose(s) of the Use or Disclosure.
- b) Uses and Disclosures Permitted By Law. As permitted by the Privacy Rule, Business Associate may:
 - b.i) Use PHI: as is necessary for the proper management and administration of Business Associate’s organization; to provide data aggregation services relating to the health care services of the Covered Entity; and to carry out the legal responsibilities of Business Associate.
 - b.ii) Disclose PHI if the disclosure is Required By Law; or is subject to reasonable assurances obtained by Business Associate from the third party to whom the PHI is disclosed that PHI will be held confidentially, securely, and Used or Disclosed only as Required By Law or for the purposes for which it was disclosed to such third party, and any breaches of confidentiality of PHI which become known to such third party will be promptly reported to Business Associate.
- c) Privacy Rule. To the extent Business Associate carries out one or more of Business Entity’s obligations under the Privacy Rule, Business Associate shall comply with the requirements of HIPAA that apply to Business Entity in the performance of such obligation(s).
- d) Safeguards. Business Associate shall use appropriate and sufficient safeguards to prevent Use or Disclosure of PHI other than the Uses and Disclosures permitted or required by this BAA. Business Associate shall comply with the Security Rule with

respect to EPHI, including implementing Administrative Safeguards, Physical Safeguards, and Technical Safeguards that reasonably and appropriately protect the Confidentiality, Integrity and Availability of EPHI.

- e) Reporting. Business Associate shall promptly report, but no later than ten (10) days after discovery, to Business Entity any Use or Disclosure of PHI not permitted or required by the Terms of Access and any Security Incident of which it becomes aware in accordance with HIPAA. The parties agree that this section constitutes notice by Business Associate to Business Entity of the ongoing existence and occurrence of attempted Unsuccessful Security Incidents. “Unsuccessful Security Incidents” shall include, but not be limited to, pings and other broadcast attacks on Business Associate’s firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of PHI.
- f) Agents and Subcontractors. Business Associate shall ensure that any and all subcontractors that create, receive, maintain or transmit PHI on behalf of Business Associate agree, in writing prior to the subcontractors’ receipt of such PHI, to the same terms and conditions of this BAA with respect to PHI. Each subcontract agreement must contain the same restrictions and conditions applying to Business Associate with respect to PHI, including without limitation the provisions of this BAA. Business Associate shall make such agreements with its subcontractors available to Business Entity upon Business Entity’s request.
- g) Patient Rights.
 - g.i) Access and Amendment. Business Associate does not expect to maintain a Designated Records Set under the Services. However, to the extent that Business Associate maintains a Designated Record Set, Business Associate shall:
 - (g.iii.1) Notify Business Entity as promptly as reasonably practicable upon receipt of a request from an Individual for access to or a copy of such Individual’s PHI or to amend such Individual’s PHI;
 - (g.iii.2) Make PHI available to Business Entity, as reasonably requested by Business Entity and in accordance with 45 C.F.R. § 164.524 to enable Business Entity to respond to the Individual’s request for access; and
 - (g.iii.3) Upon receipt of notice from Business Entity, promptly amend any portion of the PHI so that Business Entity may meet its amendment obligations under 45 C.F.R. § 164.526.
 - g.ii) Patient Right to Request Accounting. Business Associate shall document and make available to Business Entity the information required to provide an accounting of disclosures within ten (10) days of receipt of Business Entity’s request or, as directed by Business Entity, to the subject of the PHI, in compliance with the requirements of 45 C.F.R. §164.528. If any Individual requests an accounting from Business Associate, Business Associate shall, within two (2) business days, notify Business Entity of the

details of such request. Business Associate agrees to implement an appropriate record keeping process to enable it to comply with the requirements of this Section.

- h) Audit. Business Associate shall make its internal practices, books, and records relating to the Use and Disclosure of PHI received from, or created or received by Business Associate on behalf of Business Entity available to the Secretary of Health and Human Services, upon request, solely for purposes of determining and facilitating Business Entity's compliance with HIPAA.
- i) De-identified Data. Business Associate may de-identify PHI in accordance with 45 C.F.R. § 164.514(b) and may Use or Disclose such de-identified data to the extent permitted under HIPAA and unless prohibited by applicable law. Business Associates shall have the rights to the use and ownership of the De-Identified Data as set forth in the Terms of Access.
- j) Mitigation. Business Associate shall mitigate promptly, to the extent practicable, any harmful effect that is known to Business Associate of a Use or Disclosure of PHI by Business Associate in violation of this BAA, the Privacy Rule, the Security Rule, or other applicable federal or state law.
- k) Breach. If Business Associate has knowledge or a reasonable belief a Breach of Unsecured Protected Health Information has occurred, Business Associate shall notify the Business Entity within fifteen (15) days of discovery. Such notification shall include, to the extent possible, the identification of each Individual whose PHI has been or is reasonably believed to have been accessed, acquired, Used or Disclosed during the Breach, along with any other information that the Business Entity will be required to include in its notification to the Individual, the media and/or the Secretary and a description of the Business Associate's investigation, mitigation, and prevention efforts.

4. Business Entity Obligations.

- a) Notice of Privacy Practices. Business Entity shall notify Business Associate of limitation(s) in its notice of privacy practices to the extent such limitation affects Business Associate's permitted Uses or Disclosures.
- b) Individual Permission. Business Entity shall notify Business Associate of changes in, or revocation of, permission by an Individual to Use or Disclose PHI, to the extent such changes affects Business Associate's permitted Uses or Disclosures.
- c) Restrictions. Business Entity shall notify Business Associate of restriction(s) in the Use or Disclosure of PHI that Business Entity has agreed to, to the extent such restriction affects Business Associate's permitted Uses or Disclosures.

5. Term & Termination.

- a) Term. The Term of this BAA shall begin on the Effective Date, and shall continue until all PHI provided by Business Entity to Business Associate is destroyed or returned to Business Entity. If it is infeasible to return or destroy all PHI, this BAA shall continue for so long as PHI is maintained by Business Associate, which maintenance shall be in accordance with Section 4(c) herein.

- b) Termination.
 - b.i) By Business Entity. Upon determination by Business Entity, in its reasonable discretion, of a material breach by Business Associate of this BAA, Business Entity may terminate this BAA upon thirty (30) days' notice; provided however, Business Entity shall not terminate if Business Associate takes reasonable steps to mitigate harm resulting from the breach and otherwise agrees to comply with the terms of this BAA on a forward-looking basis within such thirty (30) day notice period.
 - b.ii) By Business Associate. Upon determination by Business Associate, in its reasonable discretion, of a material breach by Business Entity of the Terms of Access, Business Associate may terminate this BAA upon thirty (30) days' notice; provided however, Business Associate shall not terminate if Business Entity takes reasonable steps to mitigate harm resulting from the breach and otherwise agrees to comply with the terms of this BAA on a forward-looking basis within such thirty (30) day notice period.
 - c) Return on Termination. At termination of this BAA, the Terms of Access or the Business Entity's right to access the Platform, to the extent feasible, Business Associate shall return or destroy all PHI Business Associate maintains in any form and shall retain no copies of PHI, except for PHI that has been De-identified such that it no longer protected under HIPAA. Notwithstanding anything herein to the contrary, if Business Associate determines, in its reasonable discretion, the return or destruction of such PHI is not feasible, Business Associate shall extend the protections of this BAA to the remaining information and limit further Uses and Disclosures of PHI to those purposes that make the return or destruction of PHI infeasible.
 - d) Survival. The terms of this Section shall survive the termination or expiration of this BAA.
6. Required Disclosure. If Business Associate is confronted with legal action to disclose any PHI, Business Associate shall, to the extent permitted, promptly notify Business Entity of such action. Thereafter, upon request by Business Entity, Business Associate shall use reasonable efforts to assist Business Entity in obtaining a protective order or other similar order, and shall disclose only the minimum amount of PHI that is required to be disclosed in order to comply with the legal action, whether or not a protective order or other order has been obtained.
7. Compliance with Laws. Business Associate shall comply with all applicable federal, state and local laws, rules and regulations. To the extent that Business Entity's operations constitute a "Part 2 Program" as defined in the federal alcohol and drug rehabilitation regulations at 42 C.F.R. Part 2 ("**Part 2**"), and PHI provided to Business Associate contains "records" as defined in 42 C.F.R. § 2.11 ("**Substance Use Disorder Records**"), Business Associate acknowledges that, with respect to Substance Use Disorder Records and in receiving, storing, processing, or otherwise dealing with Substance Use Disorder Records, Business Associate is fully obligated and bound to comply with Part 2. Business Associate (i) shall use, disclose, and release Substance Use Disorder Records in accordance with Part 2, and (ii) if necessary, will resist in judicial proceedings any efforts to obtain access to Substance Use Disorder Records and patient identifying information related to substance use disorder diagnosis, treatment, or referral for

treatment except as permitted by Part 2. With respect to the Part 2 Program, Business Associate also will be a qualified service organization as defined under Part 2.

8. Conflict. Except as specifically required to implement the purposes of this BAA, and except to the extent inconsistent with this BAA, all terms of the Terms of Access shall remain in full force and effect. In the event of a conflict between the terms of the Terms of Access and this BAA, this BAA shall control. This BAA supersedes any and all other agreements between the parties related to this subject matter.
9. No Third-Party Beneficiaries. Nothing express or implied in this BAA is intended to confer, nor shall anything herein confer, upon any person other than the Business Entity, Business Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.
10. Amendment. This BAA is subject to change. Subject to applicable law, Business Associate may amend this BAA from time to time by posting the revised BAA on the Platform and/or otherwise making Business Entity aware of the changes. Business Entity's continued use of the Platform following our notice of changes to this BAA (or other method of legal acceptance) signifies acceptance of such changes. Please refer to the "Last updated" date above to see when this BAA was last updated.