



**HIPAA
BUSINESS ASSOCIATE AGREEMENT**

THIS HIPAA BUSINESS ASSOCIATE AGREEMENT (the “Agreement”) is entered into on the last date of signature below by and between _____, a _____ corporation (“Covered Entity), and Surescripts, LLC, a Delaware limited liability company (“Surescripts”).

WITNESSETH

WHEREAS, Congress enacted the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), that protects the confidentiality of health information;

WHEREAS, pursuant to HIPAA, the United States Department of Health and Human Services (“HHS”) promulgated Breach Notification Standards, Privacy Standards, and Security Standards (collectively, the “HIPAA Standards”), each as defined below, governing confidential health information;

WHEREAS, Surescripts performs certain services on behalf of Covered Entity;

WHEREAS, Covered Entity and Surescripts have entered into one or more contractual relationships (the “Underlying Agreement(s)”) which require Surescripts to create, receive, maintain, or transmit Protected Health Information on Covered Entity’s behalf; and

WHEREAS, in order to comply with the Business Associate requirements of HIPAA and its implementing regulations, Surescripts and Covered Entity must enter into an agreement that governs the Uses and Disclosures of such Protected Health Information by Surescripts.

NOW, THEREFORE, in consideration of the foregoing recitals, the mutual promises and covenants set forth herein, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. Definitions. For purposes of this Agreement, the following words shall have the following meanings.

“Breach” when capitalized, “Breach” shall have the meaning set forth in 45 C.F.R. § 164.402; with respect to all other uses of the word “breach” in this Agreement, the word shall have its ordinary contract meaning.

“Breach Notification Standards” shall mean the Breach Notification for Unsecured Protected Health Information Rule, 45 C.F.R. Parts 160 and 164, Subparts A and D, as currently in effect.

“Electronic Health Record” shall have the meaning set forth in Section 13400(5) of the HITECH Act, which is defined as an electronic record of health-related information on an Individual that is created, gathered, managed and consulted by health care clinicians and staff.

“HITECH Act” shall mean the Health Information Technology for Economic and Clinical Health Act, found in Title XIII of the American Recovery and Reinvestment Act of 2009, effective February 17, 2009.

“Individual” shall have the same meaning as set forth in 45 C.F.R. § 160.103, defined as the person who is the subject of Protected Health Information, and shall include a personal representative in accordance with 45 C.F.R. § 164.502(g).

“Privacy Standards” shall mean the Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Parts 160 and 164, Subparts A and E, as currently in effect.

“Protected Health Information” or **“PHI”** shall have the meaning set forth at 45 C.F.R. § 160.103 for “protected health information” except that, for purposes of this Agreement, Protected Health Information and all variations of the term (including Electronic Protected Health Information, PHI and Unsecured Protected Health Information) shall be limited to information that Surescripts creates, receives, maintains, or transmits on behalf of Covered Entity.

“Secretary” shall mean the Secretary of the U.S. Department of Health and Human Services or any office or person within the U.S. Department of Health and Human Services to which/whom the Secretary has delegated his or her authority to administer the HIPAA Standards, such as the Director of the Office for Civil Rights.

“Security Standards” shall mean Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. Part 160 and Part 164, Subparts A and C.

Capitalized terms used but not defined herein shall have the meanings ascribed to them in the HIPAA Standards.

2. **Surescripts Obligations.** Surescripts shall comply with the following terms of this Agreement.

2.1 Permitted Uses and Disclosures.

2.1.1 Except as otherwise limited in this Agreement, Surescripts may Use and Disclose PHI as necessary to fulfill its responsibilities under the Underlying Agreement(s) and as otherwise specifically requested by Covered Entity, so long as such Use or Disclosure would not violate the Privacy Standards if done by the Covered Entity, and provided that Surescripts is notified in writing by Covered Entity of additional limitations on Uses or Disclosures.

2.1.2 Except as otherwise limited in this Agreement, Surescripts may Use PHI for its proper management and administration, to fulfill its legal responsibilities, or as Required by Law. Surescripts may Disclose PHI in its possession to third parties for its proper management and administration (that may include, without limitation, Disclosure to connected participants regarding a potential Known Misuse [as such term is defined in Section 2.5 below] that may impact the connected participant and their operations) or to fulfill any of its legal responsibilities, but only if (i) the Disclosure is Required by Law, or (ii) Surescripts has received written assurances from the third party that 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 third party and that the third party will notify Surescripts of any instances of which it is aware in which the confidentiality of the PHI has been breached.

2.1.3 Surescripts may Use PHI in its possession to provide Data Aggregation services relating to the Health Care Operations of Covered Entity or, if Covered Entity is a Business Associate, for the Covered Entity on whose behalf Covered Entity is acting.

2.1.4 Consistent with the requirements of 45 C.F.R. § 164.502(j)(1), Surescripts may Disclose PHI to report conduct that is unlawful or otherwise violates professional or clinical standards, or that care, services, or conditions potentially endangers one or more patients, workers, or the public.

2.1.5 Surescripts agrees to make reasonable efforts to limit the Use and/or Disclosure of PHI to the minimum necessary to accomplish the intended purpose of the Use, Disclosure, or request in accordance with 45 C.F.R. §§ 164.502(b) and 164.514(d) and any guidance issued by the Secretary.

2.1.6 Surescripts will not Use or Disclose PHI other than as permitted or required by this Agreement or as Required by Law.

2.2 Disclosures to Subcontractors. Surescripts shall ensure that any Subcontractors that create, receive, maintain, or transmit PHI on Surescripts' behalf have entered into an agreement containing the same terms and conditions as set forth in this Agreement, including that the Subcontractor shall comply with the applicable requirements of the Security Standards.

2.3 Appropriate Safeguards. Surescripts shall implement appropriate administrative, technical, and physical safeguards to prevent any Use or Disclosure of PHI not authorized by this Agreement.

2.4 Compliance with Security Standards. Surescripts shall comply with the applicable requirements of the Security Standards.

2.5 Reporting of Illegal, Unauthorized, or Improper Uses or Disclosures and Remedial Actions. Surescripts shall report to Covered Entity any illegal, unauthorized, or improper Use or Disclosure of PHI, Security Incident, or Breach of Unsecured PHI (collectively, "Known Misuse") by it within thirty (30) business days of obtaining knowledge of such Known Misuse. In the case of a Breach of Unsecured PHI, the initial notice will contain all relevant information available to Surescripts at the time such notice is provided. Without unreasonable delay and within sixty (60) calendar days following discovery of any Breach of Unsecured PHI by Surescripts, Surescripts shall provide Covered Entity a notice containing all information required to be included in such notice pursuant to 45 C.F.R. § 164.410(c). Surescripts shall take commercially reasonable actions to mitigate the negative impact of any Known Misuse and adopt additional or improve existing safeguards to prevent recurrence. To the extent that Surescripts transmits PHI on Covered Entity's behalf, the parties acknowledge that Surescripts shall have no obligation to report any impermissible Use or Disclosure or Security Incident by the recipient of the PHI, unless the recipient is acting on Surescripts' behalf.

Notwithstanding the preceding, the parties acknowledge and agree that this section constitutes notice by Surescripts to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which no additional notice to Covered Entity shall be required. "Unsuccessful Security Incidents" shall include, but not be limited to, pings and other broadcast attacks on Surescripts' 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.

2.6 Internal Practices, Books, and Records. Surescripts shall make its internal practices, books, and records relating to the Use and Disclosure of PHI received from or created or received by Surescripts on behalf of Covered Entity available to the Secretary, or the Secretary's designees, for purposes of determining Surescripts' and Covered Entity's compliance with the Privacy Standards. Nothing in this Section shall be construed as a waiver of any legal privilege or of any protections for trade secrets or confidential commercial information by Surescripts.

2.7 Access to PHI. Surescripts is not subject to the right of access under 45 C.F.R. § 164.524 because Surescripts does not maintain PHI in a Designated Record Set. Surescripts shall notify Covered Entity within five (5) business days of receiving a request from an Individual to access PHI. Following receipt of such notice from Surescripts, Covered Entity shall handle such request from the Individual.

2.8 Amendments to PHI. Surescripts is not subject to the right of amendment under 45 C.F.R. § 164.526 because Surescripts does not maintain PHI in a Designated Record Set. Surescripts shall notify Covered Entity within five (5) business days of receiving a request from an Individual to amend PHI. Following receipt of such notice from Surescripts, Covered Entity shall handle such request from the Individual.

2.9 Accounting of Disclosures.

2.9.1 Within twenty (20) business days of a request by Covered Entity, Surescripts shall provide Covered Entity with an accounting of all Disclosures of PHI as necessary to permit Covered Entity to comply with its obligations under 45 C.F.R. § 164.528 to provide Individuals with an accounting of Disclosures of their PHI.

2.9.2 Surescripts shall notify Covered Entity within five (5) business days of receiving a request from an Individual for an accounting of Disclosures of PHI. Following receipt of such notice from Surescripts, Covered Entity shall handle such request from the Individual.

2.9.3 In accordance with the HITECH Act, the parties acknowledge that the Secretary shall promulgate regulations regarding the right of Individuals to receive an accounting of Disclosures made for Treatment, Payment and Health Care Operations during the previous three (3) years if such Disclosures are made through the utilization of an Electronic Health Record. The parties agree to comply with such regulations promulgated by the Secretary as of the effective date of those regulations.

3. Covered Entity Obligations.

3.1 Notice of Privacy Practices. To the extent that Covered Entity is a Covered Entity that is required to provide to Individuals a notice of privacy practices pursuant to 45 C.F.R. § 164.520, Covered Entity shall ensure, throughout the term of this Agreement, that such notice adequately describes all the

Uses and Disclosures of PHI that Surescripts is allowed to make pursuant to this Agreement. To the extent that Covered Entity is a Business Associate, Covered Entity shall notify Surescripts of any applicable limitation(s) of which Covered Entity is aware in the notice of privacy practices of a Covered Entity under 45 C.F.R. § 164.520 to the extent such limitation(s) may affect Surescripts Use or Disclosure of PHI under this Agreement.

3.2 Individual Permission. Covered Entity shall notify Surescripts of changes in, or revocation of, permission by an Individual to Use or Disclose PHI of which Covered Entity is aware to the extent such changes affect Surescripts' permitted Uses or Disclosures of PHI under this Agreement.

3.3 Restrictions. Unless legally required to do so, Covered Entity shall not agree to restrictions on Use or Disclosure, as provided for in 45 C.F.R. § 164.522, of PHI to the extent such restrictions affect Surescripts' Permitted Uses or Disclosures of PHI under this Agreement without the express written consent of Surescripts and without holding Surescripts harmless from the adverse financial and business costs associated with any such agreement. If Covered Entity is legally required to agree to a restriction on Use or Disclosure of PHI, Covered Entity shall notify Surescripts of any such restriction to the extent such restriction affects Surescripts' Uses or Disclosures of PHI under this Agreement.

3.4 Consents and Authorizations. Covered Entity represents and warrants that any and all consents, authorizations, or other permissions necessary under the Privacy Standards or other applicable law (including state law) to perform the services under the Underlying Agreement(s) or this Agreement have been properly secured.

3.5 Impermissible Requests. Covered Entity shall not request Surescripts to Use or Disclose PHI in any manner that would not be permissible under the Privacy Standards if done by Covered Entity, except for Uses or Disclosures set forth in Sections 2.1.2 and 2.1.3 above.

4. Term and Termination.

4.1 Term. The Term of this Agreement shall commence on and this Agreement shall be effective as of the date of the Underlying Agreement(s). This Agreement shall terminate in accordance with the terminations provisions of this Agreement and the Underlying Agreement(s).

4.2 Termination for Cause. In the event either party determines that the other has breached a material term of this Agreement, including engaging in a pattern of activity or practice that constitutes a material breach of a term of this Agreement, and such violation continues for thirty (30) calendar days after written notice of such breach has been provided, the party claiming a breach shall have the right to terminate the Underlying Agreement(s) for cause.

4.3 Effect of Termination.

4.3.1 Return or Destruction of PHI; Disposition When Return or Destruction Not Feasible. Upon termination of this Agreement, the parties hereby acknowledge that the return or destruction of PHI received by Surescripts from Covered Entity is not feasible and that, therefore, Surescripts may retain a copy of such PHI. The provisions of this Agreement shall continue to apply to any such PHI retained following cancellation, termination, expiration, or other conclusion of the Underlying Agreement(s), and

Surescripts shall limit Uses and Disclosures of such PHI to those purposes that make the return or destruction thereof not feasible for as long as Surescripts maintains such PHI.

4.3.2 Reasonable Fees. All reasonable fees incurred to cause the return, destruction, or storage of PHI under this Section 4.3 shall be borne by the Covered Entity.

5. Miscellaneous.

5.1 Regulatory References. A reference in this Agreement to a section in HIPAA, the HITECH Act, or the HIPAA Standards means the section as in effect or as amended at the time.

5.2 Survival. The respective rights and obligations of the parties under Section 4.3 of this Agreement shall survive the termination of this Agreement.

5.3 Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the parties to comply with the HIPAA Security Standards. Except to the extent specified by this Agreement, all of the terms and conditions of the Underlying Agreement(s) shall be and remain in full force and effect. In the event of any inconsistency or conflict between this Agreement and the Underlying Agreement(s), the terms and provisions and conditions of this Agreement shall govern and control.

5.4 Amendment. The parties shall work together through reasonable negotiations to amend this Agreement as necessary to comply with any changes in law, including, but not limited to, the promulgation of amendments to the HIPAA Standards required by the HITECH Act or any other future laws, applicable to or affecting the rights, duties, and obligations of the parties under this Agreement or the Underlying Agreement(s).

5.5 Independent Relationship. None of the provisions of this Agreement are intended to create, nor will they be deemed to create, any relationship between the parties other than that of independent parties contracting with each other as independent contractors solely for the purposes of effecting the provisions of this Agreement and the Underlying Agreement(s).

5.6 Notices. All notices and notifications under this Agreement shall be sent in writing by traceable carrier to the listed persons on behalf of Surescripts and Covered Entity at the addresses indicated on the last page hereof, or such other address as a party may indicate by at least ten (10) calendar days' prior written notice to the other party. Notices will be effective upon receipt.

5.7 Construction and Jurisdiction. This Agreement shall be governed by and construed in accordance with the laws of the Commonwealth of Virginia (excepting any conflict of laws provisions which would serve to defeat application of Virginia law). Each of the parties hereto submits to the exclusive jurisdiction of the state and/or federal courts located within the Commonwealth of Virginia for any suit, hearing, or other legal proceeding of every nature, kind, and description whatsoever in the event of any dispute or controversy arising hereunder or relating hereto, or in the event any ruling, finding, or other legal determination is required or desired hereunder.

5.8 Limitation of Liability. Neither Party shall be liable to the other Party for any incidental, consequential, special, or punitive damages of any kind or nature, whether such liability is asserted on the basis of contract, tort (including negligence or strict liability), or otherwise, even if the other Party has been advised of the possibility of such loss or damages.

5.9 No Third Party Beneficiaries. Nothing express or implied in the Underlying Agreement or this Agreement is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Surescripts, and their respective successors or assigns any rights, remedies, obligations, or liabilities whatsoever.

5.10 Counterparts. This Agreement may be executed in two or more counterparts, each of which shall be an original, but all of which taken together shall constitute one and the same agreement.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement to be effective as of the last date set forth below.

COVERED ENTITY:

SURESCRIPTS, LLC

**(Insert legal name of entity as it appears on
Incorporation documents)**

Covered Entity warrants, represents, covenants, and agrees that the individual executing the Agreement on behalf of Covered Entity has been duly authorized to act for and bind Covered Entity.

By: _____
(authorized signature)

By: _____

Print Name: _____

Name: Thomas M. Farah

Title: _____

Title: SVP, General Counsel

Date: _____

Date: _____

Names and Addresses for Notices Under this Business Associate Agreement

FOR COVERED ENTITY

FOR SURESCRIPTS, LLC

Name

Title

Address for Notices

Address for Notices

Privacy Officer

Title

2800 Crystal Drive, 10th Floor

Address for Notices

Arlington, VA 22202

Address for Notices