



BUSINESS ASSOCIATE AGREEMENT

This Exhibit B, Business Associate Agreement (“Agreement”), is effective upon execution and is made a part of the _____ dated as of _____, 201__ (“Underlying Agreement”) by and between _____ (“Business Associate”) and Rush University Medical Center (“Rush” or “Covered Entity”).

RECITALS

WHEREAS, Covered Entity and Business Associate acknowledge and agree that the execution and delivery of this Agreement is necessary and desirable in order for Covered Entity to comply with the requirements of the implementing regulations at 45 Code of Federal Regulations (“CFR”) Parts 160 and 164, Subparts A and E (the “Privacy Rule”) and Part 164, Subparts A and C (the “Security Rule”) for the Administrative Simplification provisions of Title II, Subtitle F of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”); and

WHEREAS, Covered Entity and Business Associate acknowledge that the parties must meet the requirements of the HIPAA Privacy and Security Rules and Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act (“ARRA”) (Pub. L. 111-5) also known as the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”) and that under § 13404 of the HITECH Act (42 U.S.C. § 17934), its use and disclosure of PHI must be in compliance with the terms of this Agreement pursuant to 45 C.F.R. § 164.504(e).

NOW THEREFORE, for and in consideration of the recitals herein above set forth and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, Business Associate and Covered Entity hereby agree as follows:

Section I. Definitions

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy Rule or the Security Rule.

Section II. Obligations and Activities of Business Associate

- a) Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by this Agreement or as Required By Law.
- b) Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.
- c) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.
- d) Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.

- e) Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions consistent with the requirements of the HIPAA Privacy and Security Rules, and applicable provisions of the HITECH Act that apply through this Agreement to Business Associate with respect to such information.
- f) Business Associate agrees to provide access, at the request of Covered Entity, within five (5) business days of receiving such request, to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR 164.524. This provision is not applicable if Business Associate does not have Protected Health Information in Rush's Designated Record Set.
- g) Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR 164.526 within ten (10) business days of receiving such request. This provision shall not apply if Business Associate does not have Protected Health Information in Rush's Designated Record Set.
- h) Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Covered Entity, and/or to the Secretary, within five (5) business days of receiving such request, or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule and the Security Rule.
- i) Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.
- j) Business Associate agrees to provide to Covered Entity or an Individual, within ten (10) business days of receiving such request, information collected in accordance with Section II (i) of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.
- k) Business Associate agrees to implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the Electronic Protected Health Information that it creates, receives, maintains or transmits on behalf of Covered Entity. Business Associate agrees to render Electronic Health Information unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the HHS Secretary. Business Associate shall report to Covered Entity any successful unauthorized access, use, disclosure, modification or destruction of Electronic Protected Health Information or interference with system operations in an information system containing Electronic Protected



Health Information and report the aggregate number of unsuccessful, unauthorized attempts to access, use, disclose, modify or destroy Electronic Protected Health Information or interfere with system operations in an information system containing Electronic Protected Health Information, provided that: (i) such reports will be provided only as frequently as the parties mutually agree, but no more than once per month; and (ii) if the definition of “Security Incident” under the Security Rule is amended to remove the requirement for reporting “unsuccessful” attempts to use, disclose, modify or destroy Electronic Protected Health Information, the portion of this Section II(k) addressing the reporting of unsuccessful, unauthorized attempts will no longer apply as of the effective date of such amendment.

- l) Business Associate shall implement the Security Rule requirements set forth in 45 C.F.R. §§ 164.308, 164.310, 164.312, and 164.316 and acknowledges that these requirements shall apply to Business Associate in the same manner as they are applied to the Covered Entity.
- m) Business Associate agrees to notify Covered Entity without unreasonable delay and no more than ten (10) days after the discovery of a “breach” (as defined in 45 C.F.R. § 164.402) of “unsecured” (as defined in 45 C.F.R. § 164.402) Protected Health Information. Business Associate agrees to treat a breach as discovered on the first day on which the Business Associate, an employee, officer, or an agent knew of the breach or should have known of the breach if it had exercised due diligence. Business Associate shall coordinate with the Covered Entity to (i) investigate the breach, (ii) inform all affected Individuals and (iii) mitigate the breach. Business Associate shall be responsible for any and all costs associated with responding to and mitigating breaches under this Section, including but not limited to mailing costs, personnel costs, attorneys’ fees, and other related expenses or costs. Business Associate will, at a minimum, provide Covered Entity with the following information in each notification in accordance with 45 C.F.R. 164.404:
 - i. A brief description of what occurred with respect to the breach, including, to the extent known, the date of the breach and the date on which the breach was discovered;
 - ii. A description of the types of unsecured PHI that were disclosed during the breach.

Section III. Permitted Uses and Disclosures by Business Associate

(a) Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.



(b) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

(c) Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(d) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services, if applicable, to Covered Entity as permitted by 42 CFR 164.504(e)(2)(i)(B).

(e) Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with Sec. 164.502(j)(1).

(f) Except as otherwise set forth in this Agreement, Business Associate shall utilize a Limited Data Set, if practicable, for all uses, disclosures or requests of PHI. Otherwise, any uses or disclosures of PHI shall be limited to the “Minimum Necessary,” as defined in 45 C.F.R. § 164.514(d) and pursuant to the requirements set forth in the HITECH Act at § 13405(b). Business Associate acknowledges its obligation under § 13405(b)(2) (42 U.S.C. § 17935(b)(2)) of the HITECH Act to determine what constitutes the minimum necessary to accomplish the intended purposes of any disclosure of PHI.

Section IV. Obligations of Covered Entity

(a) Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR 164.520, to the extent that such limitation may affect Business Associate’s use or disclosure of Protected Health Information.

(b) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate’s use or disclosure of Protected Health Information.

(c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate’s use or disclosure of Protected Health Information.

Section V. Permissible Requests by Covered Entity

Covered Entity shall not request or Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity. In the event that Agreement is for the provision of data aggregation services, Business Associate may provide data aggregation services relating to the health care operations of Covered Entity. Business Associate may use and disclose Protected Health Information for its own management and administration pursuant to Sections III (b) and (c) of this Business Associate Agreement.



Section VI. Term and Termination

(a) **Term.** This Agreement shall be effective upon execution, and shall terminate when all of the Protected Health Information 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 Rush agrees with Business Associate that it is infeasible to return or destroy Protected Health Information as set forth and further described in Section VI(c)(2), protections are extended to such information, in accordance with the termination provisions in this Section VI.

(b) **Termination for Cause.** Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

(1) Provide an opportunity for Business Associate to cure the breach within five (5) days of receiving notice of the breach or end the violation and terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

(2) Immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible; or

(3) If neither termination nor cure are feasible, Covered Entity shall report the violation to the Secretary.

(c) **Effect of Termination.**

(1) Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

(2) In the event that Business Associate and Covered Entity determine that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity written notification of the conditions that make return or destruction infeasible. Upon Rush's receipt of written notification from Business Associate that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

Section VII. Miscellaneous

(a) **Regulatory References.** A reference in this Agreement to a section in the Privacy Rule or the Security Rule means the section as in effect or as amended.

(b) **Amendment.** The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity and Business Associate to comply with the requirements of the HITECH Act, the Privacy Rule, the Security Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.



(c) **Survival.** The respective rights and obligations of Business Associate under Section VI and VII of this Agreement shall survive the termination of this Agreement.

(d) **Interpretation.** Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the HITECH Act, the Privacy Rule and the Security Rule.

IN WITNESS WHEREOF, Rush and _____ have caused this Agreement to be executed by duly authorized officers as of the day and year first written above.

BUSINESS ASSOCIATE

RUSH UNIVERSITY MEDICAL CENTER

By: _____

By: _____

Its: _____

Its: _____