HIPAA Business Associate Agreement – Sample Notice

Disclaimer: Template Business Associate Agreement (45 C.F.R. § 164.308)

The information provided in this document does not constitute, and is no substitute for, legal or other professional advice. Users should consult their own legal or other professional advisors for individualized guidance regarding the application of the law to their particular situations, and in connection with other compliance-related concerns.

Business Associate Agreement

This Business Associate Agreement ("Agreement") is entered into this ___ day of _____, _____ between [name of Covered Entity], a [state name][professional corporation] [partnership] [sole proprietorship] ("Physician Practice") and [name of Business Associate], a [type of business entity] ("Contractor").

RECITALS

Physician Practice is a [type of organization] that provides medical services with a principal place of business at [address].

Contractor is a [type of organization] that [description of primary functions or activities] with a principal place of business at [address].

Physician Practice, as a Covered Entity under the Health Information Portability and Accountability Act of 1996 ("HIPAA") is required to enter into this Agreement to obtain satisfactory assurances that Contractor, a Business Associate under HIPAA, will appropriately safeguard all Protected Health Information ("PHI") as defined herein, disclosed, created, maintained or received by Contractor on behalf of Physician Practice.

Physician Practice desires to engage Contractor to perform certain functions for, or on behalf of, Physician Practice involving the disclosure of PHI by Physician Practice to Contractor, or the

creation, maintenance or use of PHI by Contractor on behalf of Physician Practice, and Contractor desires to perform such functions.

This contract shall be deemed an amendment to the parties' underlying contract dated _____ ("Underlying Agreement").

In consideration of the mutual promises below and the exchange of information pursuant to this agreement and in order to comply with all legal requirements for the protection of this information, the parties therefore agree as follows:

Article I. Definitions of Terms

1.01 "Agreement" means this Business Associate Agreement.

1.02 "Business Associate" shall have the meaning given to such term in 45 C.F.R. § 160.103.

1.03 "C.F.R." shall mean the Code of Federal Regulations.

1.04 "Covered Entity" shall have the meaning given to such term in 45 C.F.R. § 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Covered Entity].

1.05 "Designated Record Set" shall have the meaning given to such term in 45 C.F.R. § 164.501.

1.06 "Electronic Protected Health Information or Electronic PHI" shall have the meaning given to such term under the Privacy Rule and the Security Rule, including, but not limited to, 45 C.F.R. § 160.103, as applied to the information that Business Associate creates, receives, maintains or transmits from or on behalf of Physician Practice.

1.07 "HIPAA Rules" shall mean the Privacy, Security, Breach Notification and Enforcement Rules at 45 C.F.R. Parts 160

and 164.

1.08 "Individual" shall have the same meaning given to such term in 45 C.F.R. § 160.103 and shall include a person who qualifies as the individual's personal representative in accordance with 45 C.F.R. § 164.502(g).

1.09 "Privacy Rule" shall mean the Privacy Standards at 45 C.F.R. Part 164, Subpart E.

1.10 "Protected Health Information" ("PHI") shall have the meaning given to such term in 45 C.F.R. § 160.103.

1.11 "Required By Law" shall have the same meaning given to such term in 45 C.F.R. § 164.103.

1.12 "Secretary" shall mean the Secretary of Health and Human Services ("HHS") or his or her designee as provided in 45 C.F.R. § 160.103.

1.13 "Security Incident" shall have the same meaning given to such term under the Security Rule, including, but not limited to, 45 C.F.R. § 164.304.

1.14 "Security Rule" shall mean the Security Standards at 45 C.F.R. Part 164, Subparts A and C.

Article II. Obligations and Activities of Contractor

2.01 Protected Health Information. Contractor agrees and acknowledges that any individual's Protected Health Information that comes within Contractor's custody, exposure, possession or knowledge or is created, maintained, retained, transmitted, derived, developed, compiled, prepared or used by Contractor in the course of or in connection with the performance of services under this Agreement, is confidential and shall remain the exclusive property of Physician Practice and shall be used, disclosed, transmitted and/or maintained solely in accordance with this Agreement and as

Required By Law. Contractor agrees to comply with its obligations as a Business Associate and acknowledges that it is subject to and agrees to comply with HIPAA and all applicable guidance and regulations issued by the Secretary to implement HIPAA and all other applicable law.

2.02 Use of Protected Health Information. Contractor shall not use or disclose Protected Health Information other than as permitted or required by this Agreement or as Required By Law.

2.03 Forwarding Requests for Disclosure from Government to Physician Practice. Contractor shall forward all requests for the disclosure of Protected Health Information from a law enforcement or government official, or pursuant to a subpoena, other legal request or court or administrative order, to Physician Practice as soon as possible before making the requested disclosure, but no later than five (5) business days following its receipt of such request or order.

2.04 Assisting Physician Practice Respond to Requests for Disclosure from Government. Contractor shall provide to Physician Practice all Protected Health Information necessary to respond to a request for the disclosure of Protected Health Information by a law enforcement or government official, or pursuant to a subpoena, other legal request, or court or administrative order as soon as possible, but no later than two (2) business days following its receipt of such written request from Physician Practice.

2.05 Restrictions on Use and/or Disclosure of Protected Health Information. Contractor shall comply with all granted restrictions on the use and/or disclosure of Protected Health Information, pursuant to 45 C.F.R. § 164.522(a), upon notice from Physician Practice. Contractor shall forward to Physician Practice any requests for restriction on the use and/or disclosure of Protected

Health Information within five (5) business days of receipt.

2.06 Requests for Confidential Communication of Protected Health Information. Contractor shall comply with all granted requests for confidential communication of Protected Health Information, pursuant to 45 C.F.R. § 164.522(b), upon notice from Physician Practice. Contractor shall forward to Physician Practice any requests for confidential communication of Protected Health Information within ten (10) business days of receipt.

2.07 Appropriate Safeguards. Contractor shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of the Physician Practice, as required by the Security Rule.

2.08 Duty to Mitigate. Contractor shall take immediate steps to mitigate, to the extent practicable or as reasonably directed by Physician Practice, any harmful effect that is known to Contractor of a use or disclosure of Protected Health Information by Contractor in violation of the requirements of this Agreement, the Privacy Rule or the Security Rule, such as obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed.

2.09 Reporting of Unauthorized Uses or Disclosures. Contractor shall report to Physician Practice any use or disclosure of the Protected Health Information not provided for by this Agreement, the Privacy Rule or the Security Rule, including breaches of unsecured Protected Health Information, as required at 45 C.F.R. § 164.410, and any security incident of which it becomes aware, as soon as possible, but no later than five (5) business days after discovery, stating (to the extent known by Contractor) the nature of such use or disclosure, the names and addresses of the individuals

who are the subject of such Protected Health Information and the names of the individuals who made or engaged in such use or disclosure and any other available information that the Physician Practice is required to include in notifications to the affected individuals.

2.10 Subcontractors, Consultants, Agents and Other Third Parties. Contractor shall in accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2) ensure that any subcontractor, consultant, agent, or other third party that creates, receives, maintains, or transmits Protected Health Information on behalf of Contractor agrees to the same restrictions, conditions, and requirements that apply to Contractor with regard to its creation, use, and disclosure of Protected Health Information. Contractor shall, upon request from Physician Practice, provide Physician Practice with a list of all such third parties. Contractor shall ensure that any subcontractor, consultant, agent, or other third party to whom it provides Electronic Protected Health Information agrees to implement reasonable and appropriate safeguards to protect such information. Contractor must terminate its agreement with any subcontractor, consultant, agent or other third party, and obtain all Protected Health Information provided to such subcontractor, consultant, agent or other third party, if Contractor becomes aware that the subcontractor, consultant, agent or other third party has breached its contractual duties relating to HIPAA or this agreement. If any subcontractor, consultant, agent, or other third party of Contractor are not subject to the jurisdiction or laws of the United States, or if any use or disclosure of Protected Health Information in performing services under the Agreement will be outside of the jurisdiction of the United States, such entities must agree by written contract with the Contractor to be subject to the jurisdiction of the Secretary, the laws and the courts of the United States, and waive any available jurisdictional defenses as they pertain to the parties' obligations under this Agreement, the

Privacy Rule or the Security Rule.

2.11 Books and Records. Contractor shall make internal practices, books, and records relating to Protected Health Information received from, or created or received by Contractor, on behalf of Physician Practice, available to Physician Practice, or at the request of Physician Practice to the Secretary, for purposes of the Secretary determining Physician Practice's compliance with the Privacy Rule.

2.12 Documenting Disclosures. Contractor shall document such disclosures of Protected Health Information and information related to such disclosures as would be required for Physician Practice to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528.

2.13 Accounting for Disclosures. Contractor shall provide to Physician Practice, upon request and in the time and manner required by 45 C.F.R. § 164.528(c)(1), an accounting of disclosures of an Individual's Protected Health Information, collected in accordance with Section 2.11 of this Agreement, to permit Physician Practice to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528.

2.14 Minimum Necessary. Contractor acknowledges that it shall request from the Physician Practice and so disclose to its affiliates, subsidiaries, agents, subcontractors or other third parties, only the minimum Protected Health Information necessary to perform or fulfill a specific function required or permitted hereunder. Contractor acknowledges that the Secretary is required by the Health Information Technology for Economic and Clinical Health "HITECH Act" to issue guidance on what constitutes "minimum necessary" for purposes of the Privacy Standards. Contractor agrees to comply with the guidance, once issued by the Secretary,

and to only request, use or disclose the minimum amount of Protected Health Information as described in such guidance.

2.15 Training. Contractor shall provide training as to the Privacy Rule and the Physician Practice's privacy policy to all of its employees who will handle or be responsible for handling Protected Health Information on the Physician Practice's behalf.

2.16 Independent Contractor. The relationship of the Contractor with Physician Practice shall be one of independent contractor, and not an employee or agent of Physician Practice.

2.17 Securing Protected Health Information. Contractor will comply with Section II.B of the April 27, 2009 HHS guidance (74 Fed. Reg. 19006 at 19009-19010) setting forth the technologies and methodologies for rendering Protected Health Information unusable, unreadable, or indecipherable to unauthorized individuals such that breach notification is not required. Contractor shall insure that any subcontractor, consultant, agent, vendor, or other third party to whom it provides Protected Health Information will implement, in a reasonable and appropriate manner, the technologies and methodologies the HITECH Act and HHS guidance specifies with respect to rendering Physician Practice's Protected Health Information unusable, unreadable or indecipherable to unauthorized individuals.

2.18 Breach Notification. Notwithstanding paragraph 2.17 above, if any Protected Health Information in the possession, custody or control of Contractor remains or becomes unsecured, Contractor shall, following discovery of a breach (as such term is defined in 45 C.F.R. § 164.402) of such unsecured Protected Health Information, provide the notifications to individuals, the media and the Secretary, as set forth in 45 C.F.R. §§ 164.404 through 164.408.

2.19 Timeliness of Notifications. Except where a law enforcement

official states to Physician Practice or Contractor that a notification would impede a criminal investigation or cause damage to national security, all notifications shall be made without unreasonable delay and in no case later than 60 calendar days from discovery of the breach.

2.20 Indemnification. Contractor shall defend, indemnify and hold harmless the Physician Practice from and against any or all cost (including but not limited to any and all costs incurred by Covered Entity in complying with the breach notification requirements of 45 C.F.R. Part 164, Subpart D), loss, interest, damage, liability, claim, legal action or demand by third parties, (including costs, expenses and reasonable attorney fees on account thereof) arising out of Contractor's activities under the Agreement, including but not limited to, any breach of unsecured Protected Health Information by the Contractor or failure by the Contractor to provide the breach notifications required by 45 C.F.R. §§ 164.404 through 164.408, except to the extent that such loss, interest, damage, liability, claim, legal action or demand was incurred as a result of the negligence or willful misconduct of Physician Practice. As a condition precedent to the Contractor's obligation to indemnify Physician Practice under this Agreement, Physician Practice must notify Contractor within a reasonable amount of time upon learning of any claim or liability in order to give Contractor an opportunity to present any appropriate defense on behalf of Physician Practice and Contractor. Physician Practice shall have the right, but not the obligation, to participate in any defense at its own cost and with its own counsel. The provisions of this paragraph 2.20 will survive the termination of this Agreement.

2.21 Application of Privacy Rule to Contractor. Where provided, the standards, requirements, and implementation specifications adopted under 45 C.F.R. Part 164, Subpart E, apply to Contractor with respect to the Protected Health Information of Physician Practice.

2.22 Fundraising. Contractor agrees to clearly and conspicuously provide any recipient of fundraising communications the opportunity to opt out of receiving any further such solicitations.

2.23 Sale of Protected Health Information. Contractor shall, except pursuant to and in compliance with 45 C.F.R. § 164.508(a)(4), not engage in the sale of Protected Health Information.

2.24 Compliance and Enforcement. Contractor is subject to the compliance, enforcement and civil monetary penalties provisions at 45 C.F.R., Part 160, Subparts C and D.

2.25 Individual's Access to Protected Health Information. Contractor shall cooperate with Physician Practice on a timely basis, consistent with 45 C.F.R. § 164.524(b)(2), to fulfill all requests by individuals for access to the individual's Protected Health Information that are approved by Physician Practice. Contractor shall make available Protected Health Information in a designated record set to Physician Practice as necessary to satisfy Physician Practice's obligations under 45 C.F.R. § 164.524(c). Contractor further agrees that to the extent Contractor maintains Protected Health Information of Physician Practice in an electronic health record ("EHR"), Physician Practice must comply with patients' requests for access to their Protected Health Information by giving them, or any entity that they designate clearly, conspicuously and specifically, the information in an electronic format, and must not charge the requestor more than the labor costs in responding to the request for the copy (or summary or explanation).

2.26 Implement Information Security Program. Contractor shall implement a documented information security program that includes administrative, technical and physical safeguards designed to prevent the accidental or otherwise unauthorized use or disclosure of Protected Health Information, and the integrity and

availability of electronic Protected Health Information it creates, receives, maintains or transmits on behalf of Physician Practice. The security program shall include reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, and other requirements of the HIPAA Security Rule. In addition, Contractor agrees to (1) maintain written documentation of its policies and procedures, and any action, activity or assessment which the HIPAA Security Rule requires to be documented, (2) retain this documentation for 6 years from the date of its creation or the date when it last was in effect, whichever is later, (3) make this documentation available to those persons responsible for implementing the procedures to which the documentation pertains, and (4) review this documentation periodically, and update it as needed in response to environmental or operational changes affecting the security of the electronic Protected Health Information. Contractor agrees to encrypt all electronic Protected Health Information and destroy all paper Protected Health Information such that it is unusable, unreadable, or indecipherable to unauthorized users. Upon request, Contractor shall make available Contractor's security program, including the most recent electronic Protected Health Information risk analysis, policies, procedures, security incidents and responses and evidence of training.

2.27 Amendments to Protected Health Information. Contractor shall make any amendment(s) to Protected Health Information in a designated record set as directed or agreed to by Physician Practice pursuant to 45 C.F.R. § 164.526, or take other measures as necessary to satisfy Physician Practice's obligations under 45 C.F.R. § 164.526. Contractor must act on an individual's request for an amendment in a manner and within the time period set forth in 45 C.F.R. § 164.526(b)(2).

2.28 Marketing. Contractor shall not use or disclose Protected Health Information for marketing purposes without the

individual's authorization, except as provided in 45 C.F.R. §§ 164.508(a)(3)(i)(A) and (B).

Article III. Permitted Uses and Disclosures by Contractor

3.01 General Use and Disclosure. Except as otherwise limited in this Agreement, Contractor may use or disclose Protected Health Information only to perform its obligations and services to Physician Practice or as Required By Law, provided that such use or disclosure would not violate the Privacy or Security Rule if done by Physician Practice.

3.02 Specific Use and Disclosure Provisions.

3.02.01 Management and Administration of Contractor. Except as otherwise limited in this Agreement, Contractor may use Protected Health Information for the proper management and administration of the Contractor or to carry out the legal responsibilities of the Contractor.

3.02.02 Other Uses and Disclosures. Except as otherwise limited in this Agreement, and notwithstanding Section 3.01 above, Contractor may disclose Protected Health Information for the proper management and administration of the Contractor, provided that disclosures are Required by Law, or Contractor obtains reasonable assurances from the person to whom the information is disclosed that it will be held 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 Contractor of any instances of which it is aware in which the confidentiality of the information has been breached.

3.02.03 Data Aggregation Services. Contractor may use Protected Health Information to provide data aggregation services to Physician Practice as permitted by 42 C.F.R. §

164.504(e)(2)(i)(B).

3.02.04 Reporting Violations of the Law. Contractor may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. § 164.51(f) .

3.02.05 Reporting to Health Plan. Contractor will not disclose Protected Health Information to a health plan if the individual to whom the Protected Health Information pertains has so requested and (1) the disclosure would be for the purposes of payment or health care operations, and not for the purposes of treatment, (2) the Protected Health Information at issue pertains to a health care item or service for which the individual pays out-of-pocket and in full and (3) the disclosure is not required by law.

3.02.06 Minimum Necessary. Contractor will, in the performance of its obligations and services to Physician Practice make reasonable efforts to use, disclose and request only the minimum amount of Physician Practice's Protected Health Information reasonably necessary to accomplish the intended purpose of the use, disclosure or request, except as set forth in 45 C.F.R. § 164.502(b)(2).

Article IV. Obligations of Physician Practice

4.01 Provisions for Physician Practice to Inform Contractor of Privacy Practices and Restrictions.

4.01.01 Upon Contractor's request, Physician Practice shall provide Contractor with the notice of privacy practices that Physician Practice produces in accordance with 45 C.F.R. § 164.520, as well as any changes to that notice.

4.01.02 Physician Practice shall provide Contractor with

any changes in, or revocation of, authorization by an Individual to use or disclose Protected Health Information, if such changes affect Contractor's permitted or required uses and disclosures.

4.01.03 Physician Practice shall notify Contractor, in writing, of any restriction to the use or disclosure of Protected Health Information that Physician Practice has agreed to in accordance with 45 C.F.R. § 164.522, and Contractor agrees to conform to any such restriction.

4.01.04 Physician Practice acknowledges that it shall provide to, or request from, the Contractor only the minimum Protected Health Information necessary for Contractor to perform or fulfill a specific function required or permitted hereunder.

4.01.05 Physician Practice shall take immediate steps to mitigate an impermissible use or disclosure of Protected Health Information from Contractor to Physician Practice, including its staff, employees and agents who send and receive Protected Health Information to and from Contractor in the course and scope of their employment, such as obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means between Physician Practice and its staff, employees and agents) or will be destroyed.

4.02 Permissible Requests by Physician Practice

Physician Practice represents and warrants that it has the right and authority to disclose Protected Health Information to Contractor for Contractor to perform its obligations and provide services to Physician Practice. Physician Practice shall not request Contractor to use or disclose Protected Health Information in any

manner that would not be permissible under the Privacy Rule if done by Physician Practice.

Article V. Term and Termination

5.01 Term. The provisions of this Agreement shall take effect _____. Except as otherwise provided herein, the Agreement shall terminate when all of the Protected Health Information provided by Physician Practice to Contractor, or created or received by Contractor on behalf of Physician Practice, is destroyed or returned to Physician Practice.

5.02 Termination for Cause. Upon a Party's knowledge of a material breach by the other party, the non-breaching Party shall provide an opportunity for the breaching Party to cure the breach or end the violation and terminate this Agreement if the breaching Party does not cure the breach or end the violation within the time specified by the non-breaching Party or immediately terminate this Agreement if cure of such breach is not possible.

5.03 Termination Without Cause. Either party to this Agreement may terminate the Agreement upon provision of [sixty (60)] days prior written notice.

[NOTE: Ensure the notice period is long enough to allow for replacement of the services.]

5.04 Effect of Termination.

5.04.01 Disposal of PHI. Except as provided in paragraph 5.04.02 of this Section, upon termination of this Agreement, for any reason, Contractor shall return or destroy all Protected Health Information received from Physician Practice, or created or received by Contractor on behalf of Physician Practice, at the direction of Physician Practice. Contractor shall request, in writing, Protected Health Information that is in the possession of subcontractors or

agents of Contractor.

5.04.02 In the event the Contractor determines that returning or destroying the Protected Health Information is infeasible, Contractor shall provide to Physician Practice notification of the conditions that make return or destruction infeasible. If return or destruction of Protected Health Information is infeasible, Contractor shall extend the protection of this Agreement to such Protected Health Information, for so long as Contractor maintains such Protected Health Information. Following the termination of this Agreement, Contractor shall not disclose Protected Health Information except to Physician Practice or as Required by Law.

Article VI. Miscellaneous

6.01 Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

6.02 Amendment. This Agreement may be amended upon the mutual written agreement of the parties. Upon the enactment of any law or regulation affecting the use or disclosure of Protected Health Information, or the publication of any decision of a court of the United States or any state relating to any such law or the publication of any interpretive policy or opinion of any governmental agency charged with the enforcement of any such law or regulation, either party may, by written notice to the other party, and by mutual agreement, amend the Agreement in such manner as such party determines necessary to comply with such law, policy, decision or regulation. If the other party disagrees with such amendment, it shall so notify the first party in writing within thirty (30) days of the notice. If the parties are unable to agree on an amendment within thirty (30) days thereafter, then either of the parties may terminate the Agreement on thirty (30)

days written notice to the other party.

6.03 Survival. The obligations of Contractor under Section 5.04.02 of this Agreement shall survive the termination of this Agreement.

6.04 Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Physician Practice to comply with the HIPAA Rules. In the event of any inconsistency or conflict between this Agreement and any other agreement between the parties, the terms, provisions and conditions of this Agreement shall govern and control. In the event of an inconsistency between the provisions of the Agreement and the mandatory terms of the HIPAA Rules, as may be amended from time to time by HHS or as a result of interpretations by HHS, a court, or another regulatory agency with authority over the Parties, the interpretation of HHS, such court or regulatory agency shall prevail. In the event of a conflict among the interpretations of these entities, the conflict shall be resolved in accordance with rules of precedence. Where provisions of this Agreement are different from those mandated by the HIPAA Rules, but are nonetheless permitted by the HIPAA Rules, the provisions of the Agreement shall control.

6.05 No third party beneficiary. Nothing express or implied in this Agreement is intended to confer, and nothing herein shall confer, upon any person other than the parties and the respective successors or assigns of the parties, any rights, remedies, obligations, or liabilities whatsoever.

6.06 Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the State of Illinois. Any disputes relating to this Agreement shall be resolved by the state or federal courts located in Chicago, Illinois, and Contractor consents to venue in those courts as proper.

IN WITNESS WHEREOF, the parties hereto have duly executed this agreement to be effective as of [effective date of the agreement].

Physician Practice

By: _____

Name: _____

Title: _____

Date: _____

Contractor

By: _____

Name: _____

Title: _____

Date: _____