HIPAA BUSINESS ASSOCIATE AGREEMENT

This Agreement dated as of _____is made by and between _____ (hereinafter referred to as "**Covered Entity**") and _____ (hereinafter referred to as "**Business Associate**"), collectively the Parties.

PREAMBLE

This Agreement governs the terms and conditions under which Business Associate will access Protected Health Information (PHI) belonging to patients of Covered Entity in performing services for, or on behalf of, Covered Entity.

SECTION 1 - DEFINITIONS

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in 45 CFR 160.103 and 164.501, and the final rule issued on January 17, 2013, effective March 26, 2013. For purposes of this section:

1.1 Breach. "Breach" shall have the same meaning as the term "breach" in 45 CFR 164.402.

1.2 Designated Record Set (DRS). A group of records maintained by or for a Covered Entity as defined in 45 CFR 164.501.

1.3 Electronic Protected Health Information, EPHI or Electronic PHI. "Electronic Protected Health Information", "EPHI" or "Electronic PHI" shall have the same meaning as the term "electronic protected health information" in 45 CFR §160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

1.4 HIPAA. HIPAA shall mean the Health Insurance Portability and Accountability Act of 1996, as it may be amended from time to time, and the HIPAA Rules and Regulations and any other pertinent regulations which may be issued by the U.S. Department of Health and Human Services.

1.5 HIPAA Rules and Regulations. "HIPAA Rules and Regulations" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

1.6 Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

1.7 Privacy Rule. "Privacy Rule" shall mean 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 HITECH Act.

1.8 Protected Health Information or PHI. "Protected Health Information" or "PHI" shall have the same meaning as the term "protected health information" in 45 CFR 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

1.9 Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR 164.103.

1.10 Secretary. “Secretary” shall mean the Secretary of the Department of Health and Human Services or his/her designee.

1.11 Security Incident. "Security Incident" shall have the meaning set forth in 45 CFR 164.304: "[T]he attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."

1.12 Security Rule. “Security Rule” shall mean the security standards at 45 CFR Part 160 and 164 Subparts A and C, as amended by the HITECH Act.

1.13 Subcontractor. “Subcontractor” shall have the same meaning as the term “subcontractor” in 45 CFR 160.103.

1.14 Underlying Agreement. “Underlying Agreement” shall mean all agreements and relationships between Covered Entity and Business Associate, whether written or verbal, pursuant to which Business Associate provides certain services to Covered Entity and, in connection with those services, Covered Entity discloses to Business Associate certain individually identifiable PHI that is subject to protection under HIPAA.

SECTION II - OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

2.1 Business Associate acknowledges that it is directly subject to the Security Rule and to certain portions of the Privacy Rule and will maintain the compliance documentation required under the HIPAA Rules and Regulations. For purposes of HIPAA, Business Associate is not an agent of Covered Entity. Business Associate agrees to:

2.1.1 Not use or disclose PHI other than as permitted or required under this Agreement or as Required by Law.

2.1.2 Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI, to prevent use or disclosure of the PHI other than as provided for by this Agreement.

2.1.3 Report in writing to Covered Entity without unreasonable delay and in no case later than 5 business days after discovery any acquisition, access, use or disclosure of the PHI not provided for by this Agreement of which it becomes aware, including breaches of unsecured PHI as required at 45 CFR 164.410. Business Associate shall fully cooperate with Covered Entity in investigating the potential or actual breach, disclosure or inappropriate access and in meeting Covered Entity’s obligations under the HITECH Act and any other state or federal privacy or security breach notification laws, including, without limitation, assisting the Covered Entity with performing a risk assessment as set forth in 45 C.F.R. §164.402(2) and providing any information and documentation related to such risk assessment to the Covered Entity promptly upon request.

2.1.4 Report in writing to Covered Entity without unreasonable delay and in no case later than 5 business days after discovery any Security Incident of which it becomes aware. Business Associate shall mitigate, to the extent practicable, any harmful effect known to Business Associate from a Security Incident. Notwithstanding the foregoing, the Parties acknowledge and agree that this Section constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined herein) for which no additional notice to Covered Entity shall be required. “Unsuccessful Security Incidents” include, but are not 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 electronic PHI.

2.1.5 In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors and agents that create, receive, maintain, or transmit PHI on behalf of Business Associate on behalf of Covered Entity agree to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such information and do not store PHI beyond the borders of the United States of America. Remote access to data stored within the borders of the United States of America is allowed as long as appropriate HIPAA technical controls are utilized. These controls must be approved by the UAB Health System Information Services (HSIS) Information Security Team. Printing of PHI beyond the borders of the United States of America is not allowed.

2.1.6 Within five (5) business days of a request by Covered Entity or the Secretary, make available PHI in a Designated Record Set to Covered Entity as necessary to satisfy Covered Entity's obligations under 45 CFR 164.524, as well as make any amendments to PHI in a Designated Record Set (and incorporate any amendments, if required) as directed or agreed to by the Covered Entity in order to meet the requirements under 45 CFR 164.526.

2.1.7 Within five (5) business days of a request by Covered Entity or the Secretary, make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received or transmitted or maintained by Business Associate on behalf of Covered Entity, to the Secretary, in a time and manner designated by Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's or Business Associate's compliance with the HIPAA Rules and Regulations. In the event such a request comes directly from the Secretary, Business Associate agrees to notify Covered Entity promptly of such request.

2.1.8 Document such disclosures of PHI 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 PHI in accordance with 45 CFR 164.528.

2.1.9 Provide to Covered Entity or an Individual, in time and manner designated by Covered Entity, information collected in accordance with this section, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR 164.528.

2.1.10 Comply with the minimum necessary requirements under the HIPAA Rules.

2.2 Encryption. Business Associate agrees to implement a mechanism to encrypt electronic PHI, or if implementing encryption is not reasonable and appropriate, document the reason for that determination and implement an equivalent alternative measure that is reasonable and appropriate under the circumstances. Notwithstanding the previous sentence, *Business Associate is required to encrypt any PHI transmitted electronically and/or stored on any type of mobile media, including lap top computers, tablet computers, smart phones and portable storage or backup media.*

2.3 To the extent Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s).

2.4 Covered Entity and Business Associate acknowledge that the 21st Century Cures Act (45 CFR Part 171) prohibits knowingly engaging in any practice that is likely to interfere with, prevent, or

discourage access, exchange, or use of electronic health information ("Information Blocking"). Business Associate shall not engage in any practice that would constitute Information Blocking, shall cooperate in good faith with Covered Entity to prevent or mitigate any practice that would constitute Information Blocking, shall make all reasonable efforts to avoid causing Covered Entity to engage in Information Blocking, and otherwise shall comply with all laws regulating Information Blocking.

SECTION III - PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

3.1 Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI, as follows:

3.1.1 As necessary to perform the services specified in the Underlying Agreement.

3.1.2 As required by law.

3.2 Except as otherwise limited in this Agreement, Business Associate may disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided the disclosures are required by law, or Business Associate obtains reasonable assurances from the person or organization to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person or organization, and the person or organization notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

3.3 Business Associate is not authorized to de-identify in accordance with 45 CFR 164.514(a)-(c), PHI received by Business Associate by or on behalf of Covered Entity; nor is Business Associate authorized to use de-identified information received from Covered Entity for a purpose not authorized by this Agreement, except with the prior written consent of the Covered Entity.

3.4 Business Associate agrees to make uses and disclosures and requests for PHI consistent with the requirements of 45 CFR 164.502(b) and 164.514(d).

3.5 Business Associate may provide data aggregation services related to the health care operations of the Covered Entity.

SECTION IV - OBLIGATIONS OF COVERED ENTITY

With regard to the use and/or disclosure of PHI by Business Associate, Covered Entity agrees:

4.1 To notify Business Associate of any limitations in the notice of privacy practices of Covered Entity under 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

4.2 To inform the Business Associate of any PHI that is subject to any arrangements permitted or required of Covered Entity under the Privacy Rule that may materially impact in any manner the use and/or disclosure of PHI by Business Associate under this Agreement, such as changes in, or revocation of, the permission by an Individual to use and disclose his or her PHI as provided for in 45 CFR 164.522 and agreed to by Covered Entity, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

4.3 That it will only provide or deliver PHI that is minimally necessary to enable Business Associate to meet its obligations under the Underlying Agreement.

SECTION V - PERMISSIBLE REQUESTS BY COVERED ENTITY

5.1 Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by Covered Entity. This section shall not apply to Business Associate's use or disclosure of PHI for management, administrative, or legal responsibilities of Business Associate.

SECTION VI - TERM AND TERMINATION

6.1 Term. The obligations set forth in this section shall be effective as of the date the first PHI is released to Business Associate pursuant to this Agreement and shall continue until all of the 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 PHI, protections are extended to such information, in accordance with the termination provisions in this Section.

6.2 Termination for Cause. Upon Covered Entity's knowledge of a violation of a term of this Agreement by Business Associate, Covered Entity shall provide an opportunity for Business Associate to cure or end the violation. Covered Entity may terminate this Agreement if Business Associate does not cure or end the violation within the time specified by Covered Entity. Termination of this Agreement for cause constitutes a material breach of the Underlying Agreement warranting its termination, regardless of any provisions to the contrary in the Underlying Agreement.

6.3 Obligations of Business Associate Upon Termination. Except as otherwise agreed to in the Underlying Agreement, upon termination of this Agreement for any reason, Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:

6.3.1 Retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

6.3.2 Return to Covered Entity [or, if agreed to by Covered Entity, destroy] the remaining PHI that the Business Associate still maintains in any form;

6.3.3 Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 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;

6.3.4 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 in Section II of this Agreement which applied prior to termination; and

6.3.5 Return to Covered Entity [or, if agreed to by Covered Entity, destroy] the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities. To the extent PHI held by Business Associate is not returned to Covered Entity or destroyed, then Business Associate shall provide reasonable access to such PHI to Covered Entity.

SECTION VII - OWNERSHIP OF INFORMATION

Covered Entity holds all right, title, and interest in and to the PHI and Business Associate does not hold and will not acquire by virtue of this Agreement or by virtue of providing goods or services to Covered Entity, any right, title, or interest in or to the PHI or any portion thereof. PHI IS PROVIDED TO BUSINESS ASSOCIATE SOLELY ON AN "AS IS" BASIS. COVERED ENTITY DISCLAIMS ALL OTHER

WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE.

SECTION VIII – LIABILITY

The parties desire to set forth their respective responsibilities for liability resulting from any breach of this Agreement, including, but not limited to, a breach of PHI. These provisions supersede any provisions to the contrary in the Underlying Agreement, including, but not limited to any indemnification and limitation of liability provisions.

8.1 Injunctive Relief. The parties expressly acknowledge and agree that a violation of a term of this Agreement, or threatened violation, by it of any provision of this Agreement by one party ("Breaching Party') may cause the other party ("Nonbreaching Party") to be irreparably harmed and that they may not have an adequate remedy at law. Therefore, the parties agree that upon such violation, or threatened violation, the Nonbreaching Party will be entitled to seek injunctive relief to prevent the Breaching Party from commencing or continuing any action constituting such violation without having to post a bond or other security and without having to prove the inadequacy of any other available remedies. Nothing in this paragraph will be deemed to limit or abridge any other remedy available to the Nonbreaching Party at law or in equity.

8.2 Responsibility. Each party to this Agreement will be and remain legally responsible for its own acts and omissions, and for those of its affiliates, employees, and agents who are involved by such party in matters related to this Agreement on such party's behalf. For purposes of this Agreement, Business Associate is not an agent of Covered Entity.

8.3 Mitigation and Costs of Breach Notification. Business Associate agrees to mitigate, 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 the requirements of this Agreement. To the extent any Breach of PHI is attributable to either: (i) a breach of the obligations under this Agreement by Business Associate or (ii) a violation of the HIPAA Rules and Regulations by Business Associate, Business Associate shall bear (a) the costs incurred by Covered Entity in complying with its legal obligations relating to such breach or violation, and (b) in addition to other damages for which Business Associate may be liable for under this Agreement, the following expenses incurred by Covered Entity in responding to such breach: (1) the cost of preparing and distributing notifications to affected Individuals, (2) the cost of providing notice to government agencies, credit bureaus, and/or other required entities, (3) the cost of providing affected Individuals with credit monitoring services to the extent the incident could lead to a compromise of the data subject's credit or credit standing, (4) call center support for such affected Individuals for a specific period not to exceed thirty (30) days from the date the breach notification is sent to such affected Individuals and (5) the cost of any other measures required under applicable law.

8.4. Insurance and Indemnification. Business Associate shall: 1) maintain and furnish Covered Entity with a Certificate of Coverage for cybersecurity insurance coverage against improper uses and disclosures of PHI by Business Associates with minimum coverage limits of $5 million; and 2) indemnify, defend, and hold Covered Entity, its employees, directors, trustees, officers, representatives and agents (collectively the Indemnitees) harmless from and against all claims, causes of action, liabilities, judgments, fines, assessments, penalties, damages, awards, or other expenses, of any kind or nature whatsoever, including, without limitation, attorneys' fees, expert witness fees, and costs of investigation, litigation, or dispute resolution, incurred by the Indemnitees and relating to or arising out of any breach of the terms of this Agreement by Business Associate or its subcontractors, agents, or representatives.

SECTION IX - MISCELLANEOUS

9.1 Regulatory References. A reference in this Agreement to a section in the HIPAA Rules and Regulations means the section as in effect or as amended, and for which Compliance is required.

9.2 Applicability. As of the Effective Date, this Agreement shall automatically amend and be incorporated as part of the Underlying Agreement, whether or not specifically referenced therein. Should there be any conflict between the language of this Agreement and the Underlying Agreement (either previous or subsequent to the date of this Agreement), the language and provisions of this Agreement shall control and prevail unless the Parties specifically refer in a subsequent written agreement to this Agreement by its title and date and specifically state that the provisions of the later written agreement shall control over this Agreement.

9.3 Construction and Interpretation. This Agreement shall be construed as broadly as necessary to implement and comply with HIPAA, the HIPAA privacy and security regulations (45 CFR 160 and 164) and Subtitle D of the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). The Parties agree that any ambiguity in this Agreement shall be resolved in favor or a meaning that complies and is consistent with HIPAA, HIPAA regulations, and the HITECH Act.

9.4 Notice. All notices and other communications required or permitted pursuant to this Agreement shall be in writing, addressed to the party at the address set forth at the end of this Agreement, or to such other address as either party may designate from time to time. All notices and other communications shall be mailed by registered or certified mail, return receipt requested, postage pre-paid, or transmitted by hand delivery or telegram. All notices shall be effective as of the date of delivery of personal notice or on the date of receipt, whichever is applicable.

9.5 Modification of Agreement. The Parties recognize that this Agreement may need to be modified from time to time to ensure consistency with amendments to and changes in applicable federal and state laws and regulations, including, but not limited to, HIPAA. The Parties agree to execute any additional amendments to this Agreement reasonably necessary for each party to comply with HIPAA. This Agreement shall not be waived or altered, in whole or in part, except in writing signed by the Parties.

9.6 Transferability. Covered Entity has entered into this Agreement in specific reliance on the expertise and qualifications of Business Associate. Consequently, Business Associate's interest under this Agreement may not be transferred or assigned or assumed by any other person, in whole or in part, without the prior written consent of Covered Entity.

9.7 Governing Law and Venue. This Agreement shall be governed by, and interpreted in accordance with, the internal laws of the State of Alabama, without regard to its conflict of laws provisions.

9.8 Binding Effect. This Agreement shall be binding upon, and shall ensure to the benefit of, the Parties hereto and their respective permitted successors and assigns.

9.9 Execution. This Agreement may be executed in multiple counterparts, each of which shall constitute an original and all of which shall constitute but one Agreement.

9.10 Gender and Number. The use of the masculine, feminine, or neuter genders and the use of the singular and plural shall not be given an effect of any exclusion or limitation herein. The use of the word "person" or "party" shall mean and include any individual, trust, corporation, partnership, or other entity.

9.11 Priority of Agreement. If any portion of this Agreement is inconsistent with the terms of the Underlying Agreement, the terms of this Agreement shall prevail. Except as set forth above, the remaining provisions of the Underlying Agreement are ratified in their entirety.

9.12 No Third Party Beneficiaries. Nothing in this Business Associate Agreement shall confer upon any person other than the Parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

9.13 Survival. The obligations of Business Associate under Section VI and Section VIII shall survive the termination of this Agreement.

COVERED ENTITY		**BUSINESS ASSOCIATE**	
By:	_____	By:	_____
Name:	_____	Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____
Email:	_____	Email:	_____
Phone:	_____	Phone:	_____

BUSINESS ASSOCIATE PRIMARY CONTACT INFORMATION (REQUIRED)

Contact's Name: _____

Title: _____

Address: _____

Phone: _____ **Fax:** _____

Email: _____ **Website URL:** _____

BUSINESS ASSOCIATE SECONDARY CONTACT INFORMATION (REQUESTED)

Contact's Name: _____

Title: _____

Address: _____

Phone: _____ **Fax:** _____

Email: _____ **Website URL:** _____