

Business Associate Agreement

This Business Associate Agreement (“Agreement”) effective _____, 20____ (the “Effective Date”), is entered into by and between _____ (“Business Associate”) and **THE FLORIDA ATLANTIC UNIVERSITY BOARD OF TRUSTEES** for the benefit of the healthcare components of Florida Atlantic University (hereinafter referred to as “University” or “Covered Entity”).

WITNESSETH:

WHEREAS, Covered Entity and Business Associate are entering into an agreement identified as the _____ (“**Business Arrangement(s)**”), pursuant to which Business Associate may provide services for Covered Entity that require Business Associate to access health information that is protected by state and/or federal law; and

WHEREAS, this Agreement and the **Business Arrangement(s)** will be executed within the mandated time so that University and Business Associate are in compliance with state and/or federal law when Business Associate, in conjunction with services to be provided, is granted access to health information that is protected by state and/or federal law; and

WHEREAS, Business Associate and University desire that Business Associate obtain access to such information in accordance with the terms specified herein.

NOW, THEREFORE, in consideration of the mutual promises set forth in this Agreement and other good and valuable consideration, the sufficiency and receipt of which are hereby severally acknowledged, the parties agree as follows:

1. **Definitions.** All capitalized terms not otherwise defined in this Agreement shall have the meanings set forth in HIPAA, the Privacy Standards, the Security Standards, and HITECH Act (as defined herein).
2. **Regulatory References.** A reference in this Agreement to a section in HIPAA, the Privacy Standards, the Security Standards, the HITECH ACT, or implementing regulations means the section as in effect or as amended, and for which compliance is required.
3. **Business Associate Obligations.** Business Associate may receive from University health information that is protected under applicable state and/or federal law, including without limitation, protected health information (“PHI”) as defined in the regulations at 45 CFR Parts 160 and 164 (the “Privacy Standards”) promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). Business Associate agrees not to use or disclose (or permit the use or disclosure of) PHI in a manner that would violate the requirements of the Privacy Standards if the PHI were used or disclosed by University in the same manner. Business Associate shall use appropriate safeguards to prevent the use or disclosure of PHI other than as expressly permitted under this Agreement or as Required by Law.
4. **Use of PHI.** Business Associate may use PHI received from University only (i) for the purpose of performing services for University as such services are defined in **Business Arrangement(s)**, and (ii) as necessary for the proper management and administration of the Business Associate or to carry out its legal responsibilities, provided that such uses are permitted under federal and state law. University shall retain all rights in the PHI not granted herein. Business Associate agrees and understands that the PHI shall be and remain the property of the Covered Entity and that Business Associate acquires no title or rights to the PHI, including any de-identified PHI, as a result of this Agreement.
5. **Disclosure of PHI.** Business Associate may disclose PHI as necessary to perform its obligations under the **Business Arrangement(s)** and as permitted by law, subject to the principle of “minimum necessary,” (reference Section 6 herein). If Business Associate discloses PHI received from University, or created or received by Business Associate on behalf of University, to agents authorized to receive, use or have access to PHI maintained, obtained or created under this Agreement, including a subcontractor (collectively, “Recipients”), Business Associate shall require Recipients to agree in writing to the same restrictions and conditions on the use and/or disclosure of PHI that apply to the Business Associate under this Agreement. To the extent permitted by law, Business Associate shall be fully liable to University for any acts, failures or omissions of Recipients in furnishing the services as if they were the Business Associate's own acts, failures or omissions. Business Associate shall report to University any unauthorized use or disclosure of PHI received from University, of which it

becomes aware, as soon as reasonably practical but not later than 10 days after Business Associate becomes aware of such use or disclosure. Business Associate agrees to mitigate, to the extent practical, any harmful effect that is known to Business Associate and is the result of a use or disclosure of PHI in violation of this agreement. Business Association shall not directly or indirectly receive remuneration in exchange for any PHI. Business Associate shall not make or cause to be made any communication about a product or service or any written fundraising communication that is prohibited by 42 U.S.C. §17936.

6. Minimum Necessary. Business Associate shall at all times comply with the “minimum necessary” requirements for use and disclosure of PHI, as defined in the Privacy Standards, Security Standards, HITECH Act, and any implementing regulations. As required by the HITECH Act, the use, disclosure, or request of PHI shall be limited, to the extent practicable, to a limited data set or, if needed, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request. In addition, the entity disclosing the PHI (as opposed to the requester) shall make the minimum necessary determination.
7. Individual Rights Regarding Designated Record Sets. If Business Associate maintains a Designated Record Set on behalf of University, Business Associate shall (a) permit an Individual to inspect or obtain a copy of PHI contained in that set about the Individual under conditions and limitations required under 45 CFR § 164.524, and (b) amend PHI maintained by Business Associate as requested by University and in accordance with the Privacy Standards set forth at 45 CFR § 164.526. Business Associate shall respond to any request from University for access by an Individual within twenty (20) calendar days of such request and shall make any amendment requested by University within forty (40) calendar days of such request. Business Associate shall notify University within five (5) calendar days of receipt of any request for access or amendment by an Individual. Business Associate shall have a process in place for requests for amendments and for appending such requests to the Designated Record Set.
8. Accounting of Disclosures. Business Associate shall make available to University in response to a request from an Individual, information required for an accounting of disclosures of PHI with respect to the Individual, in accordance with 45 CFR § 164.528, incorporating exceptions to such accounting designated under the regulation, and any additional requirements imposed by the HITECH Act and its implementing regulations. Business Associate shall provide such information necessary to provide an accounting within forty (40) calendar days of University's request.
9. Withdrawal of Consent or Authorization. Business Associate agrees, if it receives, or if Covered Entity provides notice of revocation, expiration or invalidity of patient consent for the use of PHI, to cease the use and disclosure of any such Individual's PHI except to the extent it has relied on such use or disclosure, or where an exception under the Privacy Standards expressly applies.
10. Records and Audit. Business Associate shall make available to University and to the United States Department of Health and Human Services or its agents, its internal practices, books, and records relating to the use and disclosure of PHI received from, created, or received by Business Associate on behalf of University for the purpose of determining University's compliance with the Privacy and Security Standards or any other health oversight agency, in a time and manner designated by University or the Secretary. Except to the extent prohibited by law, Business Associate agrees to notify University immediately upon receipt by Business Associate of any and all requests served upon Business Associate for information or documents by or on behalf of any and all government authorities.
11. Notice of Privacy Practices. Business Associate shall obtain University's Notice of Privacy Practices (“Notice”), electronically, at University's website, <http://www.fau.edu/hipaa>, and shall periodically check University's website for any amendments to the Notice. Business Associate agrees it will abide by the limitations of any Notice published by University. An amended Notice shall not affect permitted uses and disclosures on which Business Associate has relied prior to the issuance of such Notice.
12. Term and Termination.
 - 12.1 This Agreement shall commence on the Effective Date and shall remain in effect until terminated in accordance with the terms of this Section 12. Any termination shall not affect the respective obligations or rights of the parties arising under this Agreement prior to the effective date of termination, all of which shall continue in accordance with their terms.

- 12.2 University shall have the right to terminate this Agreement for any reason upon thirty (30) calendar days' written notice to Business Associate.
- 12.3 University, at its sole discretion, may immediately terminate this Agreement and shall have no further obligations to Business Associate hereunder if any of the following events shall have occurred and be continuing:
- a. Business Associate shall fail to observe or perform any material covenant or agreement contained in this Agreement for ten (10) calendar days after written notice thereof has been given to Business Associate by University; or
 - b. A violation by Business Associate of any provision of the Privacy Standards, Security Standards, HITECH Act, or any other applicable federal or state privacy law.
- 12.4 If University is in violation of any provision of the Privacy Standards, Security Standards, or HITECH Act, or applicable federal or state privacy law, or fails to observe or perform any material covenant or agreement contained in this Agreement for sixty (60) calendar days after written notice thereof has been given to University by Business Associate, the Business Associate shall have the option to terminate this Agreement, provided all **Business Arrangement(s)** entered into between the parties, for which this Agreement is required, are also terminated.
- 12.5 Subject to the survival terms in section 12.1, this Agreement will automatically terminate without any further action of the parties upon the termination or expiration of ALL **Business Arrangement(s)** between University and Business Associate.
- 12.6 Upon termination of this Agreement for any reason, Business Associate agrees either to return to University or to destroy all PHI received from University or otherwise through the performance of services for University, that is in the possession or control of Business Associate or its agents. In the case of information for which it is not feasible to "return or destroy," Business Associate shall continue to comply with the covenants in this Agreement with respect to such PHI and shall comply with other applicable state or federal law, which may require a specific period of retention, redaction, or other treatment. Termination of this Agreement shall be cause for University to terminate any **Business Arrangement**.
13. **Indemnification.** Business Associate will indemnify, defend and hold the State of Florida, the Florida Board of Governors, the University, its Board of Trustees, and their respective officers, directors, employees, agents, contractors, volunteers, successors and assigns harmless, from and against any and all losses, liabilities, damages, costs, penalties, claims, and expenses (including reasonable attorneys' fees and court costs) arising out of or related to the negligent act or omission of, or breach of this Agreement or the **Business Arrangement(s)** by, Business Associate or its Recipients ("Claim"). If Business Associate assumes the defense of a Claim, University shall have the right, at its expense, to participate in the defense of such Claim, and Business Associate shall not take any final action with respect to such Claim without the prior written consent of University. In addition, Business Associate shall pay any and all fines and/or administrative penalties imposed based on a breach by Business Associate of the obligations stated in this Agreement or the obligations created by HIPAA, the Privacy Standards, Security Standards, HITECH Act, or their promulgating regulations. Business Associate shall provide the University with prompt notice of any Claim that may trigger the foregoing indemnification requirements. Business Associate shall cooperate in good faith in all respects with University in connection with any request by a federal or state governmental authority for additional information and documents and any governmental investigation, complaint, action or other inquiry relating to breaches or violations of this Agreement or other litigation or investigations arising hereunder.
14. **No Warranty.** PHI is provided to Business Associate solely on an "as is" basis. University disclaims all other warranties, express or implied, including but not limited to implied warranties of merchantability, and fitness for a particular purpose.
15. **Ineligible Persons.** If applicable, Business Associate represents and warrants to University that Business Associate (including Recipients) (i) is not currently excluded, debarred, or otherwise ineligible to participate in any federal health care program as defined in 42 U.S.C. § 1320a-7b(f) ("the Federal Healthcare Programs"); (ii) has not been convicted of a criminal offense related to the provision of health care items or services and not yet been excluded, debarred, or otherwise declared ineligible to participate in the Federal Healthcare Programs, and (iii) is not under investigation or otherwise aware of any circumstances which may result in Business Associate being excluded from participation in the Federal Healthcare Programs. This shall be an ongoing representation and warranty during the term of this Agreement, and Business Associate shall

immediately notify University of any change in the status of the representations and warranty set forth in this section. Any breach of this section shall give University the right to terminate this Agreement immediately for cause.

16. Use and Disclosure in Connection with Standard Transactions. If Business Associate conducts Standard Transactions (as defined in 45 CFR Part 162) for or on behalf of University, Business Associate will comply, and will require each subcontractor involved with the conduct of such Standard Transactions to comply, with each applicable requirement of 45 CFR Part 162. If necessary to specify the duties and responsibilities of each party in conducting Standard Transactions, the parties will enter into a separate detailed trading partner agreement related to the exchange of information in electronic transactions. Business Associate, however, will not enter into, or permit its subcontractors to enter into, any trading partner agreement in connection with the conduct of Standard Transactions for or on behalf of University that: (i) changes the definition, data condition, or use of a data element or segment in a Standard Transaction; (ii) adds any data elements or segments to the maximum defined data set; (iii) uses any code or data element that is marked “not used” in the Standard Transaction’s implementation specification or is not in the Standard Transaction’s implementation specification; or (iv) changes the meaning or intent of the Standard Transaction’s implementation specification.
17. Security of Electronic-PHI. If Business Associate will receive, maintain, or transmit Electronic PHI (“EPHI”) on University’s behalf, Business Associate will also comply and will require each subcontractor involved in such activity to comply with each applicable requirement of the regulations at 45 CFR Parts 160 and 164 governing the security of EPHI (the “Security Standards”). Business Associate shall, among other requirements:
 - 17.1 Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of such EPHI including but not limited to the encryption safeguards set forth in the HITECH Act and its implementing regulations; and
 - 17.2 Ensure that any agent, including a subcontractor, to whom it provides EPHI, agrees to implement reasonable and appropriate safeguards to protect it in accordance with the Security Standards; and
 - 17.3 Keep a log of all attempted and successful Security Incidents and report to Covered Entity any successful Security Incident of which it becomes aware through its security practices, which shall include, but not be limited to, a regular review of such logs.
 - 17.4 In accordance with § 817.5681 (2) (a), Florida Statutes, Business Associate shall report to Covered Entity any Security Incident as soon as practicable, but no later than ten (10) days following the determination that EPHI was, or is reasonably believed to have been acquired by an unauthorized person. A successful Security Incident report shall identify the date and scope of the successful Security Incident, and Business Associate’s response to the successful Security Incident. Business Associate shall provide further information related to the successful Security Incident as may be reasonably requested by Covered Entity. Business Associate will also provide Covered Entity with access to the log of all unsuccessful Security Incidents upon at least thirty (30) days prior written notice.
 - 17.5 To the extent that Business Associate accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses “unsecured PHI” as defined in the HITECH Act, in addition to the notification requirements with respect to EPHI set forth herein above, Business Associate shall, as soon as possible but not later than 10 days following the discovery of a breach of such information, notify Covered Entity of such breach. Such notice shall include identification of each individual whose unsecured PHI has been, or is reasonably believed by the Business Associate to have been accessed, acquired, or disclosed during such breach.
18. HITECH Act Requirements.
 - 18.1 Overview/Effective Date. The Health Information Technology for Economic and Clinical Health Act (“HITECH Act”) and its implementing regulations impose new requirements on Business Associates with respect to privacy, security, and breach notification. The HITECH Act requirements set forth in this Agreement shall apply commencing on the date of enactment of the pertinent regulations, or such other date as may be specified in those regulations, whichever is later (“Applicable Effective Date”).
 - 18.2 Direct Compliance. Business Associate agrees to comply with all aspects of the HITECH Act. Business Associate and the Covered Entity further agree that the provisions of HIPAA and the HITECH Act that now apply directly to

business associates and that are required to be incorporated by reference in a business associate agreement, including but not limited to those requirements set forth in Subtitle D of HITECH, are incorporated into this Agreement between Business Associate and Covered Entity as if set forth in this Agreement in their entirety and are effective as of the Applicable Effective Date.

18.3 Standards to Secure Data. The HITECH Act imposes on entities covered by HIPAA and their business associates federal breach notification requirements when “unsecured” PHI is acquired by an unauthorized party. The breach notification requirements will apply to PHI in any form. PHI may be vulnerable in any of the following commonly recognized data states:

- (a) “Data in motion”: Data that is moving through a wired or wireless network;
- (b) “Data at rest”: Data that resides in databases, files, or in storage;
- (c) “Data in use”: Data that is in the process of being created, maintained, updated, or destroyed; or
- (d) “Data disposed”: Data that has been discarded or recycled.

PHI in each of these data states, with the possible exception of “data in use,” may be secured using one or more methods:

(a) Encryption (which will apply only to electronic information). Encryption of “data at rest” must satisfy National Institute of Standards and Technology (“NIST”) Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices. Valid encryption processes for “data in motion” must comply with the requirements of Federal Information Processing Standards (FIPS) 140-2. These include, as appropriate, standards described in NIST Special Publications 800-52; Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs; and may include others that are FIPS 140-2 validated; and

(b) Destruction. Destruction of PHI on paper, film, or other hard copy media must involve either shredding or otherwise destroying the PHI so that it cannot be read or reconstructed. PHI on electronic media must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

(c) Redaction is specifically excluded as a means of data destruction. Nonetheless, because redaction is an approved method of de-identification under HIPAA, information that has been “de-identified” is not subject to the breach notification requirements because such information is not protected under HIPAA.

18.4 Unsecured PHI. The following requirement shall apply to the extent that Business Associate accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses “unsecured PHI,” which is defined in the HITECH Act as not secured through the use of a technology or methodology that renders the information “unusable, unreadable, or indecipherable” to unauthorized individuals. In addition to the notification requirements with respect to EPHI set forth herein above, Business Associate shall notify Covered Entity, as soon as possible but not later than 10 days following the discovery of any unauthorized acquisition, access, use or disclosure of such unsecured PHI. Business Associate shall be considered to have discovered such activity as of the first day on which the unauthorized activity is known or, by exercising reasonable diligence, would have been known to the Business Associate. Such notice shall include identification of each individual whose unsecured PHI has been, or is reasonably believed by the Business Associate to have been accessed, acquired, or disclosed during such unauthorized activity. If Covered Entity determines the unauthorized activity by Business Associate qualifies as a Breach that triggers the HITECH breach notification requirements, then Business Associate will reimburse Covered Entity for all costs related to notifying individuals of said Breach of unsecured PHI maintained or otherwise held by Business Associate. Covered Entity, at its sole discretion, shall make the determination of whether or not the definition of “Breach” as that term is set forth in the HITECH Act, 45 CFR §164.402, has been met.

19. Red Flag Rules. If Business Associate provides services with respect to patient accounts of Covered Entity, Business Associate shall implement and follow appropriate procedures to detect, prevent, and mitigate the risk of identity theft or “Red Flags” in accordance with the “Red Flag Rules” as set forth in 16 C.F.R. § 681, et seq. (the “Red Flag Rules”), and any other applicable law, rule or regulation relating to identity theft. Upon discovery of a Red Flag, Business Associate shall promptly notify Covered Entity of same and take appropriate steps to prevent or mitigate identity theft.

20. Independent Contractors. Both parties expressly intend that with regard to the provisions of this Agreement, said parties are independent contractors. Further, it is the express intent of the parties hereto that no agent, servant, contractor, or employee assigned by Business Associate to perform the Business Associate obligations described herein shall be deemed an agent, servant, contractor, or employee of the University.
21. Miscellaneous.
- 21.1 Notice. All notices, requests, demands and other communications required or permitted to be given or made under this Agreement shall be in writing, shall be effective upon receipt or attempted delivery, and shall be sent by (i) personal delivery; (ii) certified or registered United States mail, return receipt requested; (iii) overnight delivery service with proof of delivery; or (iv) facsimile with return facsimile acknowledging receipt. 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 in the **Business Arrangement(s)**, or to such other address as either party may designate from time to time. Neither party shall refuse delivery of any notice hereunder.
- 21.2 Waiver. No provision of this Agreement or any breach thereof shall be deemed waived unless such is in writing and signed by the party claimed to have waived such provision or breach. No waiver of a breach shall constitute a waiver of or excuse any different or subsequent breach.
- 21.3 Assignment. Neither party may assign (whether by operation of law or otherwise) any of its rights or delegate or subcontract any of its obligations under this Agreement without the prior written consent of the other party. Notwithstanding the foregoing, University shall have the right to assign its rights and obligations hereunder to any entity that is an affiliate or successor of University, without the prior approval of Business Associate. In no circumstance shall Business Associate subcontract, assign, or otherwise delegate any of its responsibilities under this Agreement, or the **Business Arrangement(s)** with Covered Entity, to any entity or person not subject to the jurisdiction of the United States of America.
- 21.4 Severability. Any provision of this Agreement that is determined to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this Agreement or affecting the validity or enforceability of such remaining provisions.
- 21.5 Amendment. The parties agree to take such action to amend this Agreement from time to time, as is necessary, for Covered Entity and Business Associate to comply with the requirements of HIPAA, the Privacy Standards, the Security Standards, the HITECH Act, and any implementing regulations. Notwithstanding the foregoing, the parties agree to comply with all applicable federal and state laws, rules and regulations related to PHI or to the performance of the parties pursuant to this Agreement, including but not limited to the Privacy Standards, the Security Standards, and the HITECH Act, and regulations promulgated thereunder, as well as any and all amendments to such standards and regulations.
- 21.6 Entire Agreement. This Agreement constitutes the complete agreement between Business Associate and University relating to the matters specified in this Agreement, and supersedes all prior representations or agreements, whether oral or written, with respect to such matters. In the event of any conflict between the terms of this Agreement and the terms of the **Business Arrangement(s)** or any such later agreement(s), the terms of this Agreement shall control unless the terms of such **Business Arrangement(s)** are more strict with respect to PHI and comply with the Privacy Standards, or the parties specifically otherwise agree in writing. No oral modification or waiver of any of the provisions of this Agreement shall be binding on either party. No obligation on either party to enter into any transaction is to be implied from the execution or delivery of this Agreement. This Agreement is for the benefit of, and shall be binding upon the parties, their affiliates and respective successors and assigns. No third party shall be considered a third-party beneficiary under this Agreement, nor shall any third party have any rights as a result of this Agreement.
- 21.7 Governing Law. This Agreement shall be governed by and interpreted in accordance with the laws of the state of Florida.
- 21.8 Equitable Relief. Business Associate understands and acknowledges that any disclosure or misappropriation of any PHI in violation of this Agreement will cause University irreparable harm, the amount of which may be difficult to

ascertain, and therefore agrees that University shall have the right to apply to a court of competent jurisdiction for specific performance and/or an order restraining and enjoining any such further disclosure or breach and for such other relief as University shall deem appropriate. Such right of University is to be in addition to the remedies otherwise available to University at law or in equity. Business Associate expressly waives the defense that a remedy in damages will be adequate and further waives any requirement in an action for specific performance or injunction for the posting of a bond by University.

- 21.9 Nature of Agreement. Nothing in this Agreement shall be construed to create (i) a partnership, joint venture or other joint business relationship between the parties or any of their affiliates, or (ii) a relationship of employer and employee between the parties. This Agreement does not express or imply any commitment to purchase or sell goods or services.
- 21.10 Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same document. In making proof of this Agreement, it shall not be necessary to produce or account for more than one such counterpart executed by the party against whom enforcement of this Agreement is sought.
- 21.11 Interpretation. Any ambiguity in this Agreement shall be resolved to permit the parties to comply with HIPAA, the Privacy Standards, Security Standards, and the HITECH Act. In the event of any inconsistency or conflict between this Agreement and the **Business Arrangement(s)**, the terms and provisions and conditions of this Agreement shall govern and control.

IN WITNESS WHEREOF, the parties hereto have caused these presents to be executed in several counterparts, each of which shall be deemed an original as of the Effective Date above set forth.

BUSINESS ASSOCIATE:

FLORIDA ATLANTIC UNIVERSITY BOARD OF TRUSTEES:

By: _____

By: _____

Date: _____

Date: _____