BUSINESS ASSOCIATE AGREEMENT

THIS **BUSINESS ASSOCIATE AGREEMENT** ("BAA"), effective as of the "Effective Date" set forth below, is entered into by and between the party identified as "Covered Entity" and the party identified as "Business Associate" below:

Covered Entity:	**THE BOARD OF GOVERNORS OF MISSOURI STATE UNIVERSITY**
Business Associate:	[Insert name]
Effective Date:	[Insert date]

The parties to this BAA are committed to complying with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and the rules and regulations promulgated thereunder, as amended.

In furtherance of the foregoing, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereby agree as follows:

1. DEFINITIONS.

1.1 "HIPAA Rules" means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164, as amended. A reference in this BAA to a section in the HIPAA Rules means the section as in effect or as amended.

1.2 The following terms as used in this BAA shall have the meaning ascribed to them in the HIPAA Rules: breach, data aggregation, designated record set, disclosure, electronic media, health care operations, individual, minimum necessary, notice of privacy practices, protected health information ("PHI"), required by law, Secretary, security incident, subcontractor, unsecured protected health information, use, and workforce.

1.3 "Agreement" means each existing and future agreement entered into between Covered Entity and Business Associate from time to time, whether for related or unrelated transactions, including each agreement to which this BAA is attached or incorporated by reference.

2. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

2.1. Business Associate shall use and disclose PHI only as permitted or required by this BAA, by any underlying Agreement(s), or as required by law, and shall not authorize, enable or permit any other use or disclosure of PHI.

2.2 Business Associate shall use appropriate administrative, physical and technical safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for by this BAA and to protect against any anticipated threats or hazards to the security or integrity thereof.

2.3 In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), Business Associate shall ensure that any subcontractors that create, receive, maintain, transmit or otherwise have access to use or disclose PHI on behalf of Business Associate agree to the same restrictions, conditions and requirements that apply to Business Associate with respect to such PHI, it being understood that Business Associate shall remain jointly and severally liable for any violation of the HIPAA Rules or this BAA by its subcontractors.

2.4 The HIPAA Rules provide individuals with certain rights to access and amend their PHI maintained by the Covered Entity. As part of meeting its obligations to those individuals, Covered Entity may require cooperation from the Business Associate:

(i) Right of Access. Pursuant to 45 CFR 164.524, individuals have a right of access to inspect and obtain a copy of their PHI. Promptly and no later than ten (10) days after Covered Entity's request, in a manner designated or agreed to by Covered Entity and at no charge, Business Associate shall make available PHI in a designated record set to Covered Entity or, if designated or agreed to by Covered Entity, to the individual or the individual's designee, and shall take any other actions necessary to satisfy Covered Entity's obligations under 45 CFR 164.524. If an individual requests his or her PHI directly from Business Associate, Business Associate shall notify Covered Entity promptly and no later than five (5) days after receipt of the request.

(ii) Right to Amendment. Pursuant to 45 CFR 164.526, individuals have a right to request the amendment of their PHI. Promptly and no later than ten (10) days after Covered Entity's request, in a manner designated or agreed to by Covered Entity and at no charge, Business Associate shall make amendments to PHI in a designated record set, and shall take any other actions necessary to satisfy Covered Entity's obligations under 45 CFR 164.526. If an individual requests amendment to his or her PHI directly from Business Associate, Business Associate shall notify Covered Entity promptly and no later than five (5) days after receipt of the request.

(iii) Right to Accounting of Disclosures. Pursuant to 45 CFR 164.528, individuals have a right to receive an accounting of disclosures of their PHI made in the six years prior to the date of the request. Promptly and no later than ten (10) days after Covered Entity's request, in a manner designated or agreed to by Covered Entity and at no charge, Business Associate shall make available all information required to provide an accounting of disclosures to Covered Entity or, if designated or agreed to by Covered Entity, to the individual or the individual's designee, and shall take any other actions necessary to satisfy Covered Entity's obligations under 45 CFR 164.528. If an individual requests an accounting of disclosures directly from Business Associate, Business Associate shall notify Covered Entity promptly and no later than five (5) days after receipt of the request.

2.5 To the extent Business Associate is to carry out one or more of Covered Entity's obligations under Subpart E of 45 CFR Part 164 relating to Individually Identifiable

Health Information or PHI, Business Associate shall comply with the requirements of Subpart E that apply to Covered Entity in the performance of such obligations.

2.6 Promptly and no later than ten (10) days after the request, in a manner designated or agreed to by the Secretary or Covered Entity and at no charge, Business Associate shall make its internal policies, practices, books and records relating to the security, use and disclosure of PHI available to the Secretary, Covered Entity and/or their designee(s) for purposes of determining Covered Entity's and/or Business Associate's compliance with the HIPAA Rules and this BAA. Notwithstanding this provision, no attorney-client, work product or other legal privilege will be deemed waived by Business Associate or Covered Entity as a result of this Section.

2.7 Business Associate shall not destroy PHI unless expressly designated or directed to do so in writing by Covered Entity, and further subject to Business Associate (i) notifying Covered Entity in advance of such planned destruction; (ii) ensuring that, prior to such destruction, Covered Entity has received a copy of any PHI that it desires or is required by law to retain; and (iii) complying with the return and destruction requirements of the HIPAA Rules and this BAA.

2.8 Business Associate shall not (i) remove PHI from Covered Entity's facilities or systems, (ii) export, transfer or make available PHI outside of the United States, whether for storage, processing or otherwise, or (iii) allow workforce or subcontractors not residing in the United States to access, receive or view PHI, unless expressly authorized in writing by Covered Entity in each instance.

2.9 In connection with any visits to Covered Entity's facilities or access to Covered Entity's systems, Business Associate shall comply with all on-site and remote access rules and procedures communicated by Covered Entity, including all sign-in, badging, escort, and restricted access requirements, and shall exercise reasonable care and appropriate judgment in connection therewith.

2.10 Business Associate shall evaluate and adjust its safeguards, policies and procedures as necessary to respond to evolving security threats, keep pace with generally accepted industry standards and best practices, and comply with the HIPAA Rules and other applicable laws and regulations pertaining to the privacy, security, integrity, retention, disposal, use and disclosure of PHI. Business Associate shall promptly correct any deficiencies identified as part of internal or external monitoring, testing or auditing, and shall provide Covered Entity at no charge with copies of any audit and testing reports prepared in connection therewith.

2.11 Encryption. Business Associate shall encrypt PHI transmitted, received, processed or maintained on electronic media, both while in transit and at rest, in accordance with the guidance established under the HIPAA Rules to "Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals," as amended. Whenever feasible, Business Associate shall secure all other PHI using measures that comply with the foregoing guidance. Business Associate shall provide Covered Entity with all information and assistance necessary

to decrypt and otherwise access and use PHI that has been secured by Business Associate in one of the foregoing manners.

2.12 Indemnification. Business Associate acknowledges that it is directly subject to and responsible for ensuring its compliance with the HIPAA Rules. Business Associate shall indemnify and hold Covered Entity, its affiliates and their respective directors, officers, employees and agents harmless from and against any and all claims, demands, causes of action, investigations, liabilities, losses, damages, judgments, awards, penalties, fines, settlements, costs and expenses (including reasonable attorneys' fees, expert witness fees, court costs, and costs of investigation, notification and remediation) caused by, attributable to, or otherwise arising out of or resulting from any violation of the HIPAA Rules or other applicable law, breach of this BAA, or negligent or wrongful acts or omissions by Business Associate, its workforce or subcontractors.

2.13 Insurance. Business Associate shall, at all times, maintain liability insurance coverage, including coverage for adverse privacy and security events, covering its responsibilities provided for in this BAA on an occurrence basis in minimum amounts of One Million Dollars ($1,000,000) per occurrence and One Million Dollars ($1,000,000) annual aggregate. In the event Business Associate procures insurance coverage which is not on an occurrence basis, Business Associate shall, upon the termination of such coverage, secure a continued reporting endorsement which effectively converts such coverage to occurrence based coverage.

2.14 Notwithstanding the foregoing, Business Associate shall not be required to so report to Covered Entity during any period in which Business Associate is prevented from doing so by 45 CFR 164.412 concerning law enforcement investigations.

3. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

Subject to Business Associate's compliance with the HIPAA Rules and this BAA:

3.1 Business Associate may only use or disclose PHI as authorized by and necessary to perform the services set forth in any Agreement(s).

3.2 Business Associate may use or disclose PHI as required by law. Unless otherwise required by law, Business Associate shall notify Covered Entity promptly prior to making any such use or disclosure so that Covered Entity may, if desired, resist such disclosure or seek an appropriate protective order. If Business Associate nonetheless is required by law to use or disclose PHI, Business Associate shall limit its use or disclosure to the minimum necessary that is required by law.

3.3 Business Associate shall use, disclose and request PHI in a manner consistent with the minimum necessary requirements of the HIPAA Rules and Covered Entity's minimum necessary policies and procedures.

3.4 Business Associate shall not use or disclose PHI in a manner that would violate Subpart E of 45 CFR Part 164, relating to Individually Identifiable Health Information or PHI, if such use or disclosure was made by Covered Entity.

3.5 Data Aggregation and De-Identification. Business Associate may only use PHI to provide data aggregation services relating to the healthcare operations of Covered Entity at the request of and for the sole benefit of Covered Entity and pursuant to the de-identification requirements of 45 CFR 164.514.

3.6 If use or disclosure of PHI is based upon an individual's specific consent or authorization and (i) the individual revokes such consent or authorization, (ii) the duration of such consent or authorization has expired, or (iii) the consent or authorization is found to be defective in any manner that renders it invalid, Business Associate shall notify Covered Entity promptly and no later than ten (10) days after discovering or receiving notice of such revocation, expiration or invalidity, and shall cease all further use and disclosure of the individual's PHI that is not permitted or required in the absence of such consent or authorization.

3.7 As between Covered Entity and Business Associate, Covered Entity shall remain the sole and exclusive owner of the PHI. Business Associate does not have and shall not acquire any right, title or interest in or to the PHI, including aggregate or de-identified PHI, by virtue of this BAA or any Agreement(s), or as a result of the selection, arrangement, creation or processing thereof.

4. RESPONSIBILITIES OF COVERED ENTITY

4.1 Covered Entity shall notify Business Associate of any limitations in Covered Entity's Notice of Privacy Practices under 45 CFR 164.520, to the extent that such limitations may affect Business Associate's use or disclosure of PHI. A copy of Covered Entity's current Notice of Privacy Practices is attached as Exhibit A to this BAA.

4.2 Covered Entity shall notify Business Associate of any restrictions on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restrictions may affect Business Associate's use or disclosure of PHI.

5. NOTIFICATION OF UNINTENDED USE OR DISCLOSURE OF PHI

5.1 Business Associate shall report to Covered Entity any use or disclosure of PHI not provided for in this BAA or in violation of the HIPAA Rules or other applicable law, including any and all actual and potential breaches and security incidents (each an "unintended use or disclosure"), promptly and no later than seventy-two (72) hours after Business Associate, its workforce or any subcontractor discovers, is alerted to or otherwise becomes aware of such unintended use or disclosure. Such report shall be submitted to Covered Entity's designated Privacy Officer by both mail and email using the mailing and email addresses set forth below the signature block. Business

Associate also shall notify the person designated to receive contractual notices on Covered Entity's behalf under any Agreement(s).

5.2 Business Associate shall take all reasonable actions necessary to investigate, respond to and mitigate the harmful effects of the unintended use or disclosure. Business Associate shall provide status updates and any information and assistance requested by Covered Entity in connection therewith. Unless otherwise required by law or agreed to by the parties, it shall be the responsibility of Covered Entity to communicate with affected individual(s), the Secretary and the media information regarding the unintended use or disclosure.

5.3 Reimbursement. Where the unintended use or disclosure arises out of or results in whole or in part from the negligent or willful acts or omissions of Business Associate, its workforce or subcontractors, including any violation of the HIPAA Rules or breach of this BAA, without limiting Covered Entity's rights or remedies under the circumstances, Business Associate shall reimburse Covered Entity for all reasonable costs incurred in connection with investigating, responding to, mitigating the harmful effects of, and notifying individuals, regulators and the media concerning the unintended use or disclosure, including all legal, compliance, risk management, security, and information technology expenses, all costs of printing and postage and all credit and fraud monitoring, identity theft remediation and similar services offered to affected individuals.

6. TERM AND TERMINATION

6.1 Term. The term of this BAA shall commence as of the Effective Date first stated above, and shall continue in full force and effect until the last Agreement between Covered Entity and Business Associate terminates or expires, unless sooner terminated as provided herein.

6.2 Termination by Covered Entity. Covered Entity reserves the right to immediately terminate this BAA and/or any and all other Agreement(s) between the parties, including all future payment obligations, without termination charge or penalty, if Business Associate:

(i) violates the HIPAA Rules or breaches any material provision of this BAA and does not cure such violation or breach within fifteen (15) days after receiving written notice thereof from Covered Entity; provided, however, for grossly negligent or willful or wanton acts or omissions, or a violation or breach that is not reasonably subject to cure or poses a substantial risk of harm to Covered Entity or individuals, no such opportunity to cure need be provided;

(ii) becomes or is declared insolvent, makes a general assignment for the benefit of creditors, suffers a receiver to be appointed for it, enters into an agreement for the composition, extension, or readjustment of all or substantially all of its obligations, files a voluntary petition in bankruptcy, or has an involuntary petition in bankruptcy filed against it;

(iii) is unable to provide, upon Covered Entity's demand and within a reasonable time, reasonably satisfactory written assurances of Business Associate's ability to comply with the HIPAA Rules and this BAA;

(iv) is or becomes excluded or suspended from participation in any federal or state health care reimbursement program, or becomes the subject of any investigation which Covered Entity, in its sole discretion, believes may lead to suspension or exclusion; or

(v) experiences or announces a change in control, whether by operation of law, merger, acquisition, sale of assets or business or otherwise, that has or is likely to have a negative impact on Business Associate's operations, financial condition or ability to perform under this BAA or any Agreement(s).

6.3 Return of PHI. Promptly and no later than fifteen (15) days after the expiration or termination of this BAA or any Agreement(s), or upon Covered Entity's earlier request, at no charge, Business Associate shall return to Covered Entity and/or its designee all PHI (both paper and electronic) in Business Associate's or any subcontractor's possession. Business Associate shall return PHI in a manner designated or agreed to by Covered Entity, and shall provide all information and assistance reasonably requested by Covered Entity in connection therewith. Business Associate shall not condition receipt, access to or viewing of PHI on Covered Entity's purchase, license or continued use of proprietary software or technology of Business Associate or its subcontractors. If such proprietary software or technology is required to receive, access or view PHI, Business Associate shall provide such software or technology to Covered Entity at no charge.

6.4 Destruction of PHI. Promptly and no later than thirty (30) days after the expiration or termination of this BAA or any Agreement(s), or upon Covered Entity's earlier request (in either case only after Business Associate has returned the PHI to Covered Entity as provided in 6.3 above), at no charge, Business Associate shall destroy all PHI (both paper and electronic) in Business Associate's or any subcontractor's possession, securely dispose of such PHI in accordance with the HIPAA Rules, retain no copies or summaries thereof, and, upon Covered Entity's request, certify in writing to Covered Entity that it has complied with the foregoing requirements.

6.5 Notwithstanding the destruction requirements set forth in 6.4 above, if (i) Business Associate has an independent legal right to retain PHI, as expressly set forth in any Agreement(s) or otherwise required by law, or (ii) the destruction of PHI is not feasible, as communicated promptly and in writing by Business Associate to Covered Entity, then Business Associate may retain such PHI only for so long as such independent legal right persists or such destruction is infeasible. In either case, Business Associate may further use or disclose retained PHI only for the limited purpose that made destruction inapplicable or infeasible, and the obligations, limitations and protections of this BAA shall extend and continue to apply to such PHI.

6.6 The obligations of Business Associate and rights and remedies of Covered Entity under this BAA shall survive the expiration or termination of this BAA and/or any Agreement(s) for any reason, and shall be binding on and inure to the benefit of the parties and their respective successors and permitted assigns.

7. MISCELLANEOUS

7.1 Jurisdiction. This BAA shall be governed and interpreted for all purposes by the laws of the State of Missouri, U.S.A., without giving effect to any conflict of laws principles that would require the application of the laws of a different jurisdiction. In the event Missouri law is more restrictive than federal law, the principle of pre-emption shall apply and the state law will supersede the federal. Any dispute, action or proceeding arising out of or related to this BAA may be commenced in Greene County, Missouri or, if proper subject matter jurisdiction exists, the United States District Court for the Western District of Missouri. Each party irrevocably submits and waives any objections to the personal jurisdiction and venue of such courts.

7.2 Independent Contractor. In connection with this BAA, any Agreement(s), and any services provided under any Agreement(s), Business Associate is and shall at all times hold itself out as an independent contractor conducting business as a principal for its own account. Nothing in this BAA or any Agreement(s) is intended or shall be construed to create any agency, employment, partnership or joint venture relationship between the parties. Nothing herein provides Covered Entity with the right or authority to control the Business Associate's conduct in the course of providing services for or on behalf of Covered Entity.

7.3 Notice. All notices under this BAA shall be in writing and shall be delivered either personally or by postage prepaid registered or certified mail or express courier service, return receipt requested, to the party's address for notices set forth below the signature block. Either party may change its address for notices by providing written notice of such change to the other party in the foregoing manner.

7.4 Assignment/Transfer. Neither party may assign or transfer this BAA, in whole or in part, without the prior written consent of the other party, which consent shall not be unreasonably withheld. Notwithstanding the foregoing, (i) any assignee of any Agreement(s) shall be deemed bound by the provisions of this BAA, and (ii) Covered Entity may assign this BAA to an affiliate or to a successor in interest. Any attempted assignment or transfer in violation of the foregoing shall be null and void from the beginning and without effect.

7.5 Remedies. Business Associate acknowledges that its breach or threatened breach of any provision of this BAA would cause irreparable harm to Covered Entity, the extent of which would be difficult and impracticable to assess, and that money damages would not be an adequate remedy for such breach. Accordingly, in addition to all other remedies available at law or in equity, Covered Entity shall be entitled to obtain specific performance, temporary or permanent injunctive relief, and other equitable

relief in any court of competent jurisdiction, without the necessity of posting bond in connection therewith.

7.6 Third Party Beneficiaries. If Business Associate creates, receives, maintains, transmits or otherwise uses or discloses PHI for or on behalf of any affiliate of Covered Entity, such affiliate shall be deemed an express third party beneficiary of this BAA, with full right to enforce this BAA as though a signatory hereto, and all references to Covered Entity under this BAA shall be construed to include such affiliate. If Business Associate provides services or enters into any Agreement(s) through an affiliate, such affiliate shall be deemed directly bound by and subject to this BAA, and all references to Business Associate under this BAA shall be construed to include such affiliate. Except as set forth in this paragraph, there are no third party beneficiaries to this BAA. Without limiting the foregoing, nothing contained in this BAA is intended or shall be construed to give rise to any right, claim or cause of action, contractual or otherwise, by or on behalf of any individual.

7.7 If Business Associate provides application or data processing, hosting, storage or similar services to Covered Entity, including software as a service (SaaS), cloud computing, or cloud storage, the obligations of Business Associate and rights and remedies of Covered Entity with respect to PHI under this BAA shall apply to all financial, business, accounting, technical, creative, human resources and other data created, received, maintained, transmitted or otherwise accessed, used or disclosed by Business Associate for or on behalf of Covered Entity, and such data shall be deemed included in the definition of "PHI" for such purpose.

7.8 Amendments. The parties agree to amend this BAA as necessary to comply with the HIPAA Rules and other applicable law. Any amendment to this BAA, or waiver of any provision or breach hereof, must be in writing and signed by an authorized representative of each party. No rights or obligations shall be waived by any act, omission or knowledge of a party. Any waiver on one occasion shall not constitute a waiver on subsequent occasions.

7.9 This BAA supplements any other Agreement(s) between the parties and is enforceable standing alone or as an amendment thereto. A breach of this BAA also shall be deemed a breach of any Agreement(s). A party's obligations, rights and remedies under this BAA shall not be subject to, and are expressly excluded from, any and all limitations on liability, limitations of remedy and disclaimers set forth in any Agreement(s). In the event of any conflict between this BAA and any Agreement(s), the provisions of this BAA shall control.

7.10 Any ambiguity in this BAA shall be interpreted to permit compliance with the HIPAA Rules. If any provision of this BAA is determined to be invalid or unenforceable under applicable law, the provision shall be amended and interpreted by a court of competent jurisdiction to accomplish the objectives of such provision to the greatest extent possible under applicable law, or severed from this BAA if such amendment is not feasible, and the remaining provisions of this BAA shall continue in full force and

effect. The captions in this BAA are for reference purposes only and shall not affect the meaning or interpretation of this BAA. The term "including" means "including without limitation." The terms "herein," "hereunder," "hereto" and "hereof" refer to this BAA as a whole rather than to any particular section.

7.11 This BAA sets forth the entire agreement of Covered Entity and Business Associate and supersedes all prior and contemporaneous negotiations, understandings and agreements, written or oral, concerning the subject matter hereof. Without limiting the foregoing, this BAA expressly amends, replaces and supersedes any prior BAAs in effect between Covered Entity and Business Associate.

7.12 This BAA and any amendment hereto or waiver hereof may be signed in counterparts, each of which shall constitute an original and all of which together shall constitute one and the same instrument. Any signature may be delivered by facsimile, which shall have the same effect as an original signature.

IN WITNESS WHEREOF, the parties, intending to be legally bound, have caused this BAA to be signed by their duly authorized representatives as of the Effective Date first written above.

(SIGNATURE PAGE TO FOLLOW)

BOARD OF GOVERNORS OF MISSOURI STATE UNIVERSITY

By: _____

Print: _____

Title: _____

Address for Notices:

_____

_____

_____

_____

BUSINESS ASSOCIATE:

By: _____

Print: _____

Title: _____

Address for Notices:

_____

_____

_____

_____

Privacy Officer Contact Information:

EXHIBIT A

NOTICE OF PRIVACY PRACTICES

Effective: August 1, 2014

• Missouri State University • Missouri State University – Springfield • Missouri State University – West Plains • Missouri State University – Mountain Grove • Taylor Health and Wellness Center • Greenwood Laboratory School • Learning Diagnostic Clinic • CSD/Speech, Language, & Hearing Clinic • Physical Therapy Clinic

THIS NOTICE DESCRIBES HOW YOUR MEDICAL INFORMATION MAY BE USED OR DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

OUR PLEDGE REGARDING YOUR MEDICAL INFORMATION: This notice is intended to inform you about our practices related to the protection of your medical information. We are required by law to follow the terms of the notice that is currently in effect.

This notice will explain how we may use and disclose your medical information, our obligations related to the use and disclosure of that medical information, and your rights related to medical information we have and maintain about you. When we use the words "medical information," we mean individually identifiable health information, known as protected health information or "PHI." This notice applies to all such information about your past, present, or future health or conditions; genetic information; pharmacy and prescription records; the provision of healthcare services; and the payment for those healthcare services, whether created by our employees or your physician.

We may obtain, but we are not required to obtain, your consent for the use or disclosure of your medical information for treatment, payment, or healthcare operations. We are required to obtain your authorization for the use or disclosure of information for other specific purposes or reasons. We have listed some of the types of uses or disclosures below. Not every use or disclosure is covered, but all of the ways that we are allowed to use and disclose information will fall into one of the categories.

WHO WILL FOLLOW THIS NOTICE: Missouri State University ("MSU") facilities, departments, clinics and Affiliated Covered Entities. This includes, but is not limited to: Missouri State University; Missouri State University – Springfield; Missouri State University – West Plains; Missouri State University – Mountain Grove; Taylor Health and Wellness Center; Greenwood Laboratory School; Learning Diagnostic Clinic; CSD/Speech, Language, & Hearing Clinic; and Physical Therapy Clinic; and any new entities or facilities created or acquired by MSU in the future. This Notice also applies to all employees, physicians, allied health professionals, contractors, medical staff credentialed providers, volunteers, and students conducting internships or clinical practice.

The individuals listed above may share medical information as described in this Notice of Privacy Practices. These participants are hereinafter referred to collectively with the university as "MSU". Private physician offices may have different policies or notices regarding the physician's use and disclosure of medical information created in that physician's office.

HOW WE MAY USE AND DISCLOSE YOUR MEDICAL INFORMATION WITHOUT YOUR AUTHORIZATION:

For Treatment: We may use or disclose your medical information to provide medical treatment or services. We may need to use or disclose your information to doctors, nurses, technicians, students or other MSU personnel involved in your treatment. For example, a doctor may need to know what drugs you are allergic to before prescribing medications. Further, departments or entities throughout MSU may share your medical information to coordinate your care. For instance, the laboratory may request information to complete lab work. We may also provide your physician or a subsequent healthcare provider with copies of various reports that should assist in treating you once you are discharged from our care.

For Payment: We may use and disclose your medical information so that the treatment and services you receive from MSU or another healthcare provider may be appropriately billed, and so that payment may be collected from you, an insurance company or a third-party payer. For example, we may disclose your medical information to your insurance company about a service you received at MSU so that your insurance company can pay us or reimburse you for the service. We may also ask your insurance company for prior authorization for a service to determine whether the insurance company will cover it. We may disclose your medical information to a court of law in order to collect an unpaid account. Further, you maintain the right to require MSU or one of our providers to withhold from a health plan/insurer any information pertaining to treatment you pay for out-of-pocket, unless otherwise required by law.

For Healthcare Operations: We may use and disclose your medical information for MSU operations. These include uses and disclosures that are necessary to run MSU and make sure our patients receive quality care. These uses and disclosures include, but are not limited to the following: quality assessment and improvement activities, reviewing competence or qualifications of healthcare professionals, and reviews by external agencies for licensure, accreditation, or auditing. For example, we may disclose your medical information to outside organizations or providers in order for them to provide services to you on our behalf. We may use or disclose your medical information to evaluate our staff's performance in caring for you. Medical information about you and other patients may also be combined to allow us to evaluate whether MSU should offer additional services or discontinue other services and whether certain treatments are effective. We may also compare this information with other healthcare systems to evaluate whether we can make improvements in the care and services that we offer.

When Required By Law: When required to do so by federal, state, or local law, including those that mandate the reporting of certain types of wounds or physical injuries.

To Avert a Serious Threat to Health or Safety: We may use and disclose your medical information when necessary to prevent a serious threat to the health and safety of you, the public, or any other person. However, any such disclosure would only be to someone able to help prevent the threat.

For Organ and Tissue Donation: If you are an organ donor, we may release your medical information to organizations that handle organ procurement or organ, eye or tissue transplantation, or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplantation.

Military and Veterans: If you are a member of the armed forces, we may release your medical information as required by military command authorities or for the purpose of a determination by the Department of Veterans Affairs of your eligibility for benefits. We may also release medical information about foreign military personnel to the appropriate foreign military authority.

Workers' Compensation: When disclosure is necessary to comply with Workers' Compensation laws or purposes, we may release your medical information for workers' compensation or similar programs.

Public Health Risks: We may disclose medical information about you for public health activities. These activities generally include the following: to prevent or control disease, injury or disability; to report births and deaths; to report reactions to medications or problems with products; to notify people of product recalls; to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition; or to notify the appropriate government authority if we believe a patient has been the victim of abuse, neglect or domestic violence. We may also disclose your medical information, if directed by a public health authority, to a foreign government agency collaborating with the public health authority.

Health Oversight Activities: We may disclose your medical information to a health oversight agency for activities authorized by law. These oversight activities include audits, investigations, inspections, and licensure. These activities are necessary to monitor the healthcare system, government programs, and civil rights compliance.

Legal Proceedings: We may disclose your medical information in the course of any judicial or administrative proceeding; in response to a court order or an administrative tribunal (to the extent such disclosure is expressly authorized); in certain conditions in response to a subpoena or discovery request; or for other lawful purposes.

Criminal Activity: Consistent with applicable federal and state laws, if we believe the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of yourself or others, we may disclose your medical information. However, any such disclosure would only be to someone able to help prevent the threat.

Law Enforcement: We may release medical information if asked to do so by a law enforcement official, under the following circumstances and as otherwise allowed by law: (1) about a patient who may be the victim of a crime if, under certain limited circumstances, we are unable to obtain the patient's agreement; (2) about a death we believe may be the result of criminal conduct; (3) about criminal conduct at the facility; (4) about a patient where a patient commits or threatens to commit a crime on the premises or against MSU staff (in which case we may release the patient's name, address, and last known whereabouts); (5) in emergency circumstances, to report a crime, the location of the crime or victims, and the identity, description and/or location of the person who committed the crime; and (6) when the patient is a forensic client and we are required to share with law enforcement by Missouri statute. In the event the requested medical information is protected by 42 CFR Part 2 (a federal law protecting the confidentiality of drug and alcohol abuse treatment records), a court order is required prior to MSU releasing the information.

Relating to Decedents: We may release your medical information to the coroner or medical examiner for identification purposes, determination of cause of death or for the coroner or medical examiner to perform other duties authorized by law. We may also disclose your medical information to a funeral director, as authorized by law, in order to permit the funeral director to carry out their duties. We are further permitted to make relevant disclosures to a decedent's family and friends under essentially the same circumstances such disclosures were permitted when the patient was alive as long as MSU is unaware of an expressed preference to the contrary.

National Security and Intelligence Activities: We may release your medical information to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.

Protective Services for the President and Others: We may disclose your medical information to authorized federal officials so they may conduct investigations or provide protection to the President and other authorized persons or foreign heads of state.

Inmates: If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release your medical information to the correctional institution or law enforcement official if the release is necessary: (1) for the institution to provide you with healthcare; (2) to protect your health and safety or the health and safety of others; or (3) for the safety and security of the correctional institution.

Emergency or Disaster Events: We may use or disclose your medical information to a public or private entity authorized by law to assist in disaster relief efforts, for the purpose of coordinating care or services with such entities. This may include, but is not limited to emergency managers, fire officials, law enforcement officers, public health authorities, emergency medical services such as ambulance districts and other public works officials regarding: the numbers and locations of our patients; emergency notification contacts to expedite contact with families, legal guardians, representatives or others regarding the need for evacuation or emergency care; any special needs that justify prioritization of utility restoration such as, but not limited to, dependence on respirator or other medical equipment, phone for emergency contact, etc.; or any other information that is deemed necessary to protect the health, safety and well-being of MSU patients.

Food and Drug Administration - We may disclose your medical information to a person or company required by the Food and Drug Administration to report adverse events; product defects or problems; biologic product deviations; track products; to enable product recalls; to make repairs or replacements; or for post-marketing surveillance.

Change of Ownership: In the event MSU is sold or merged with another organization, your medical information will become the property of the new owner.

Research: We may disclose your medical information to researchers when their research has been approved by an Institutional Review Board that has reviewed the research proposal and established protocols to ensure the privacy of your information. These protocols may include a waiver of authorization that has been approved by the Institutional Review Board, Privacy Committee, or any university sponsored Institutional Review Board approved by the Food and Drug Administration. For example, a research project may involve comparing the health and recovery of all patients who received one medication to those who received another medication for the same condition. All research projects, however, are subject to a special approval process under applicable law. This process evaluates a proposed research project and its use of medical information, trying to balance the research needs with the patients' need for privacy of their medical information. Before we use or disclose medical information for research, the project will have been approved through this research approval process. We may, however, disclose medical information about you to people preparing to conduct a research project, for example, to help them look for patients with specific medical needs, so long as the medical information they review does not leave the facility.

Special Circumstances: In addition, MSU reserves the right to allow your medical information to be de-identified and aggregated by MSU or third parties in accordance with all applicable laws for such uses as research, public health activities, or other healthcare operations.

UNLESS YOU OBJECT, WE ARE PERMITTED TO MAKE THE FOLLOWING USES OR DISCLOSURES: We will use or disclose your medical information for the purposes described in this section unless you object to or otherwise restrict a particular release. You must direct your written objections or restrictions to the on-site Privacy Manager the MSU Privacy Officer identified in this Notice.

Appointment Reminders/Scheduling/Follow-up Calls: We may use and disclose medical information to contact you about an appointment, a referral visit, or to follow-up with you after a visit. We may leave a brief reminder on your answering machine or voicemail system unless you tell us not to do so.

Individuals Involved in your Healthcare: We will only disclose your medical information to a member of your family, a relative, or any other person you identify and we will limit such information to that which directly relates to that person's involvement in your care. You will be asked to provide the names of these individuals.

In an Emergency: We may use or disclose your medical information in an emergency situation. If this happens, we shall try to obtain your acknowledgement as soon as reasonably practicable after the delivery of treatment.

Communication Barriers: In the event unforeseen communications barriers prohibit us from obtaining your consent, MSU will use its professional judgment to determine the level of care provided until consent can be facilitated.

Fundraising Activities: We may use or disclose your demographic information, your health insurance status, general department of service information, treating physician information, outcome information and the dates you received treatment, as necessary, in order to contact you for fundraising activities supported by MSU. You have the right to opt out of such solicitations by notifying in writing the on-site Privacy Manager or the MSU Privacy Officer.

Available Services: We may use or disclose your medical information to provide you with information about or recommendations of possible treatment options, alternatives, health benefits or services that may interest you.

Immunization Records: We are required to obtain agreement, whether in writing or given orally, from a parent, guardian, or person acting in *loco parentis* prior to disclosing or providing proof of immunizations to an educational institution admitting a minor student. No separate written HIPAA authorization is required for this action by MSU.

ALL OTHER USES AND DISCLOSURES REQUIRE YOUR PRIOR WRITTEN AUTHORIZATION. This includes most uses and disclosures for marketing purposes, any transaction in which MSU receives direct or indirect financial remuneration in exchange for your medical information, and the sharing of psychotherapy notes. If you provide us written authorization to use or disclose your medical information, you can change your mind and revoke your authorization at any time in writing. If you revoke your authorization, we will no longer use or disclose the information. However, we will not be able to take back any disclosures that we have made pursuant to your previous authorization.

YOUR RIGHTS WITH RESPECT TO MEDICAL INFORMATION:

Right to Inspect and Copy: You may inspect and obtain a copy of your medical information contained in an electronic health record or other requested designated record set for as long as we maintain that information. A "designated record set" contains medical and billing records and any other records we use for making decisions about your treatment. If you request an electronic copy, it must be provided in the format requested or in a mutually agreed-upon format. Your request must be submitted in writing to each clinic or entity where you received treatment. A copy of the authorization to request the release of information is available from the MSU Privacy Officer at each entity. If you request a copy of the information, we may charge a reasonable fee for the costs of copying, mailing, providing any electronic media (such as a USB flash drive), or other supplies associated with your request. This same right to inspect and copy extends to Business Associates of MSU as well as their Subcontractors. We may deny your request to inspect and copy based on federal law. If you are denied access to medical information, you may request the denial be reviewed. Another licensed healthcare professional chosen by the organization will review your request and the denial. The person conducting the review will not be the person who denied your original request. We will comply with the outcome of the review.

Right to Request an Amendment: You have a right to request your medical information be amended (changed) if you believe it is incorrect or incomplete for as long as MSU keeps the information. To request an amendment, you must submit a written request to the Director of the Taylor Health and Wellness Center. This written request must include why you want the information amended and why you believe the information is incorrect or incomplete. We can deny your request if it is not in writing and if it does not include a reason why the information should be amended. We can also deny your request for the following reasons: (1) the information was not created by MSU, unless the person or entity that did create the information is no longer available; (2) the information is not part of the medical record kept by or for MSU; (3) the information is not part of the information that you would be permitted to inspect and copy; or (4) we believe the request to change is not accurate. If the request for change is denied, the request will be made a part of the medical record.

Right to an Accounting of Disclosures: You have the right to request an "accounting of disclosures." This is a list of the disclosures we make of your medical information for purposes other than treatment, payment or healthcare operations as described in this Notice. MSU is required to provide an accounting of disclosures of electronic health records and other records upon request for a period of up to 6 years. It will exclude disclosures: (1) to individuals about themselves; (2) pursuant to an authorization; (3) for national security or intelligence purposes; (4) to correctional institutions or law enforcement officials; (5) as part of a limited data set; and (6) that occurred prior to the compliance date for the covered entity. To request an accounting of disclosures, you must submit your request in writing to MSU's Privacy Officer. Your data will be provided to you within 60 days unless we notify you of circumstances that warrant delay. Your first request within a 12-month period will be free. For additional requests, we may charge you for the cost of providing the list. We will notify you of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred.

Right to Request Restrictions: You have the right to request a restriction or limitation on the medical information we use or disclose about you for treatment, payment or healthcare operations. You also have the right to request a limit on the medical information we disclose about you to someone who is involved in your care or the payment for your care. WE ARE NOT REQUIRED TO AGREE WITH YOUR REQUEST. If we do agree, we will comply with your request unless the information is needed to provide you emergency treatment. To request restrictions, you must make your request in writing to MSU's Privacy Officer. In your request, you must tell us: what information you want to limit; whether you want to limit our use, disclosure or both; and to whom you want the limits to apply (for example, disclosure to your spouse).

Right to Request Confidential Communications: You have the right to request we communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that we only contact you at work or by mail. To request confidential communications, you must make your request in writing to MSU's Privacy Officer or the on-site Privacy Manager at the entity where you are receiving treatment. We will not ask you the reason for your request. We will accommodate all reasonable requests. Your request must specify how or where you wish to be contacted.

Right to a Paper Copy of This Notice: You have the right to a paper copy of this notice. To obtain a paper copy of this Notice, contact the MSU Privacy Officer. You may also obtain a copy of this Notice at our website, http://privacy.missouristate.edu/hipaa/default.htm.

Breach: In the event MSU improperly discloses or uses your medical information in violation of federal or state law, we are required to notify you of such a breach within 60 days of the event.

Complaints: If you believe we have violated your privacy rights or have not adhered to the information contained in this Notice, you may file a complaint by putting it in writing and sending it to the MSU's Privacy Officer listed at the end of this document. You may also file a complaint with the Secretary of the U.S. Department of Health and Human Services at 1-800-368-1019 (any language) or 1-800-537-7697 (TDD), or view the web-site: http://www.hhs.gov/ocr/privacy/hipaa/complaints/. You will not be retaliated against for filing a complaint with either MSU or the U.S. Department of Health and Human Services.

CHANGES TO THIS NOTICE OF PRIVACY PRACTICES: We reserve the right to change or modify the information contained in this Notice. Any changes will be effective for any medical information we have about you and any information we might obtain. Each time you receive services from MSU, we will have available the most current copy of our Notice of Privacy Practices. The most recent version will be posted in our building and our website (http://privacy.missouristate.edu/hipaa/default.htm). Also, you can call or write our contact person, whose information is included in this Notice, to obtain the most recent version.

If you have any questions about this Notice, please contact:

[NAME], Privacy and Security Officer, Missouri State University, 901 S. National Ave., Springfield, MO 65897
Email: [INSERT EMAIL ADDRESS] or call 417-[INSERT TELEPHONE NUMBER]