

BUSINESS ASSOCIATE AGREEMENT

ONslow MEMORIAL HOSPITAL, INC.

and

(Company name)

This Business Associate Agreement (“BAA”) effective on the last signature date below, is entered into by and between _____ (Company name), a _____ (State) company, (“Company”) and Onslow Memorial Hospital, Inc., a non-profit corporation organized and existing under the laws of the State of North Carolina operating in Jacksonville, North Carolina (“Covered Entity”).

- 1. BACKGROUND AND PURPOSE.** The Parties have entered into, and may in the future enter into, one or more written agreements, that require Company to be provided with, to have access to, and/or to create Protected Health Information (the “Underlying Contract(s)”), that is subject to the federal regulations issued pursuant to the Health Insurance Portability and Accountability Act (“HIPAA”) and codified at 45 C.F.R. parts 160 and 164 (“HIPAA Regulations”). This BAA shall supplement and/or amend each of the Underlying Contract(s) only with respect to **Company’s** Use, Disclosure, and creation of PHI under the Underlying Contract(s) to allow Covered Entity to comply with sections 164.502(e) and 164.314(a)(2)(i) of the HIPAA Regulations. **Company** acknowledges that, as a business associate, it is responsible to comply with the HIPAA Security and Privacy regulations pursuant to Subtitle D of the Health Information Technology for Economic and Clinical Health Act (HITECH), including Sections 164.308, 164.310, 164.312 and 164.316 of title 45 of the Code of Federal Regulations. Except as so supplemented and/or amended, the terms of the Underlying Contract(s) shall continue unchanged and shall apply with full force and effect to govern the matters addressed in this BAA and in each of the Underlying Contract(s).
- 2. DEFINITIONS.** Unless otherwise defined in this BAA, all capitalized terms used in this BAA have the meanings ascribed in the HIPAA Regulations, provided, however, that “PHI” and “ePHI” shall mean Protected Health Information and Electronic Protected Health Information, respectively, as defined in 45 C.F.R. § 160.103, limited to the information **Company** received from or created or received on behalf of Covered Entity as Covered Entity’s Business Associate. “Administrative Safeguards” shall have the same meaning as the term “administrative safeguards” in 45 C.F.R. § 164.304, with the exception that it shall

apply to the management of the conduct of **Company's** workforce, not Covered Entity's workforce, in relation to the protection of that information.

3. **OBLIGATIONS OF THE PARTIES WITH RESPECT TO PHI.**

3.1. Obligations of Company. With regard to its Use and/or Disclosure of PHI, **Company** agrees to:

- a. not Use or Disclose PHI other than as permitted or required by this BAA or as Required By Law. [§ 164.504 (e)(2)(ii)(A)] **Company** may Use and Disclose Protected Health Information only if its Use or Disclosure is in compliance with each applicable requirement of section 164.504(e) of title 45 of the Code of Federal Regulations.
- b. use appropriate safeguards to prevent Use or Disclosure of PHI other than as provided for by this BAA. [§ 164.504 (e)(2)(ii)(B)]
- c. report to Covered Entity any Use or Disclosure of PHI not provided for by this BAA of which **Company** becomes aware. [§ 164.504 (e)(2)(ii)(C)]
- d. ensure that any agents and subcontractors to whom it provides PHI received from, or created or received by **Company** on behalf of Covered Entity agree to the same restrictions and conditions set forth in the business associate provisions of the HIPAA Regulations that apply through this BAA to **Company** with respect to such information. [§ 164.504 (e)(2)(ii)(D)]
- e. within twenty (20) days of receiving a written request from Covered Entity, make available to the Covered Entity PHI necessary for Covered Entity to respond to Individuals' requests for access to PHI about them in the event that the PHI in **Company's** possession constitutes a Designated Record Set. [§ 164.504 (e)(2)(ii)(E)] In the event any individual requests access to PHI directly from **Company**, **Company** shall within five (5) business days forward such request to the Covered Entity. Any denials of access to the PHI requested shall be the responsibility of the Covered Entity.
- f. within thirty (30) days of receiving a written request from Covered Entity, make available to the Covered Entity PHI for amendment and incorporate any amendments to the PHI in accordance with 45 C.F.R. Part 164 Subpart E ("Privacy Rule") in the event that the PHI in **Company's** possession constitutes a Designated Record Set. [§ 164.504 (e)(2)(ii)(F)]
- g. within thirty (30) days of receiving a written request from Covered Entity, make available to the Covered Entity the information required for the Covered Entity to provide an accounting of disclosures of PHI as required by the Privacy Rule. [§ 164.504 (e)(2)(ii)(G)] **Company** shall provide the Covered Entity with the following information: (i) the date of the disclosure, (ii) the name of the entity or person who received the PHI, and if known, the address of such entity or person, (iii) a brief description of the PHI disclosed, and (iv) one of the following, as applicable: (a) a brief statement of the purpose of such disclosure which includes an explanation that reasonably informs the individual of the basis for such disclosure or in lieu of such statement, (b) a copy of a written request from the Secretary of Health and Human Services to

investigate or determine compliance with HIPAA; or (c) a copy of the individual's request for an accounting. In the event the request for an accounting is delivered directly to **Company**, **Company** shall within seven (7) business days forward such request to the Covered Entity.

- h. make its internal practices, books and records relating to the Use and Disclosure of PHI available to the Secretary of HHS for purposes of determining Covered Entity's compliance with the Privacy Rule. [§ 164.504 (e)(2)(ii)(H)]
- i. upon the expiration or termination of an Underlying Contract, return to Covered Entity or destroy all PHI, including such information in possession of **Company's** subcontractors, as a result of the Underlying Contract at issue and retain no copies, if it is feasible to do so. If return or destruction is infeasible, **Company** agrees to extend all protections, limitations and restrictions contained in this BAA to **Company's** Use and/or Disclosure of any retained PHI, and to limit further Uses and/or Disclosures to the purposes that make the return or destruction of the PHI infeasible. This provision shall survive the termination or expiration of this BAA and/or any Underlying Contract. [§ 164.504 (e)(2)(ii)(I)]
- j. use reasonable commercial efforts to mitigate any harmful effect that is known to **Company** of a Use or Disclosure of PHI by **Company** in violation of the requirements of this BAA.
- k. implement Administrative Safeguards, Physical Safeguards, and Technical Safeguards ("Safeguards") that reasonably and appropriately protect the Confidentiality, Integrity, and Availability of ePHI as required by 45 C.F.R. Part 164 Subpart C ("Security Rule"). [§ 164.314 (a)(2)(i)(A)]
- l. ensure that any agent and subcontractor to whom **Company** provides ePHI agrees to implement reasonable and appropriate safeguards to protect ePHI. [§ 164.314 (a)(2)(i)(B)]
- m. report promptly to Covered Entity any successful Security Incident of which **Company** becomes aware [§ 164.314 (a)(2)(i)(C)]; provided, however, that with respect to attempted unauthorized access, Use, Disclosure, modification, or destruction of information or interference with system operations in an information system affecting ePHI, such report to Covered Entity will be made available upon written request.
- n. make its policies, procedures and documentation required by the Security Rule relating to the Safeguards available to the Secretary of HHS for purposes of determining Covered Entity's compliance with the Security Rule. [68 Fed. Reg. 8334, 8359]
- o. If **Company** accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses Unsecured Protected Health Information (as defined in HITECH Sec. 4402(h)(1)), it shall, following the discovery of a breach of such information, notify the Covered Entity of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by **Company**

to have been accessed, acquired, or disclosed during such breach. [HITECH Sec. 4402 (b)]

3.2. Permitted Uses and Disclosures of PHI. Except as otherwise specified in this BAA, **Company** may make any and all Uses and Disclosures of PHI necessary to perform its obligations under the Underlying Contract(s). Unless otherwise limited herein, **Company** may:

- a. Use the PHI in its possession for its proper management and administration and to carry out the legal responsibilities of **Company** [§ 164.504 (e)(4)(i)];
- b. Disclose the PHI in its possession to a third party for the purpose of **Company's** proper management and administration or to carry out the legal responsibilities of **Company**, provided that the Disclosures are Required By Law or **Company** obtains reasonable assurances from the third party regarding the confidential handling of such PHI as required under the Privacy Rule [§ 164.504 (e)(4)(ii)];
- c. provide Data Aggregation services relating to the Health Care Operations of the Covered Entity [§ 164.504 (e)(2)(i)(B)]; and
- d. de-identify any and all PHI obtained by **Company** under this BAA, and use such de-identified data, all in accordance with the de-identification requirements of the Privacy Rule. [§ 164.502 (d)(1)]

3.3. Obligations of Covered Entity. Covered Entity agrees to timely notify **Company**, in writing, of any arrangements between Covered Entity and the Individual that is the subject of PHI that may impact in any manner the Use and/or Disclosure of that PHI by **Company** under this BAA.

4. TERMINATION BY COVERED ENTITY. Should Covered Entity become aware of a pattern of activity or practice that constitutes a material breach of a material term of this BAA by **Company**, the Covered Entity shall provide **Company** with written notice of such breach in sufficient detail to enable **Company** to understand the specific nature of the breach. Covered Entity shall be entitled to terminate the Underlying Contract associated with such breach if, after Covered Entity provides the notice to **Company**, **Company** fails to cure the breach within a reasonable time period not less than thirty (30) days specified by Covered Entity in such notice; provided, however, that such time period specified by Covered Entity shall be based on the nature of the breach involved. [§§ 164.504 (e)(1)(ii)(A), (B) & 164.314 (a)(2)(i)(D)].

5. MISCELLANEOUS.

5.1. Interpretation. The terms of this BAA shall prevail in the case of any conflict with the terms of any Underlying Contract to the extent necessary to allow Covered Entity to comply with the HIPAA Regulations. The bracketed citations to the HIPAA Regulations in several paragraphs of this BAA are for reference only and shall not be relevant in interpreting any provision of this BAA.

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

5.3. Amendment. To the extent that any relevant provision of the HIPAA Regulations is materially amended in a manner that changes the obligations of Business Associates or Covered Entities, the Parties agree to negotiate in good faith appropriate amendment(s) to this BAA to give effect to these revised obligations.

IN WITNESS WHEREOF, each of the undersigned has caused this BAA to be duly executed in its name and on its behalf.

ONSLOW MEMORIAL HOSPITAL, INC. _____ (Company name)

By: _____

By: _____

Print Name: _____

Print Name: _____

Title: _____

Title: _____

(Date)

(Date)