Business Associate Agreement

This Business Associate Agreement is made and entered into between and among the undersigned physician or medical practice (**"Practice"**), Children's Community Physicians Association (**"CCPA"**), and the Ann & Robert H. Lurie Children's Hospital of Chicago Division of Physician Services (**"Lurie Children's")**, in regard to the potential use by CCPA and/or Lurie Children's of personally identifiable medical information maintained by Practice for certain purposes described herein. Lurie Children's and CCPA accordingly are potential "business associates" of Practice under applicable federal law. The term **"Business Associate"** will be used herein to refer to each of Lurie Children's and CCPA, and the rights and obligations of Lurie Children's and CCPA hereunder shall be independent and several, and shall not be joint obligations.

1. Definitions. Capitalized terms used in this Agreement but not otherwise defined shall have the same meaning as those terms are given in (i) the Privacy Rule or the Security Rule, as applicable and (ii) the Health Information Technology Act of 2009, 42 U.S.C. prec § 17901 (the **"HITECH Act"**) and any current and future regulations promulgated under such Act. References herein to the **"Privacy Rule"** shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E. References herein to the **"Security Rule"** shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R., part 164, subpart C. Any reference in this Agreement to the Privacy Rule, the Security Rule, or the HITECH Act means such authority as in effect or as amended, and with which compliance is required. References herein to **"Protected Health Information"** or **"PHI"** (as defined in the Privacy Rule), include Electronic Protected Health Information (**"Electronic PHI"**, as defined in the Security Rule), but shall be limited to such information received by Business Associate from Practice and/or created or maintained by Business Associate on behalf of Practice.

2. Permitted Uses and Disclosures by Business Associate. Except as otherwise expressly limited by this Agreement, Business Associate may receive, use, and disclose PHI to perform the functions, activities, and services for, or on behalf of, Practice as described and specified in this Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by Practice. Without limiting the generality of the foregoing:

(i) Business Associate may use and disclose PHI for purposes of planning, designing, implementing, and operating a clinical integration program for CCPA members, and otherwise for purposes related to Practice's membership in, and participation in the activities of CCPA, as set forth in the CCPA Membership Agreement.

(ii) Business Associate may use and disclose PHI for purposes related to the membership and participation of Practice physicians on the medical staff of Lurie Children's.

(iii) Further, Business Associate may (A) use and disclose PHI for the proper management and administration of Business Associate and to carry out the legal responsibilities of Business Associate; (B) use and disclose PHI in connection with the reporting of violations of law; and (C) use PHI to create de-identified information consistent with the standards set forth at 164 C.F.R. § 164.514. If Business Associate wish to make any other disclosures of PHI for purposes of the proper management and administration of Business Associate, Business Associate shall first obtain reasonable assurances from the person to whom the information will be disclosed that it will remain confidential and used or further disclosed only for the purpose for which it was disclosed to the person or as required by law, and that the person shall notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(iv) Further, Business Associate may use PHI to provide any services to Practice that would constitute Data Aggregation services as permitted by 42 CFR § 164.504(e)(2)(i)(B).

Business Associate agrees to limit its uses and disclosures of, and requests for, PHI (a) when practical, to the information making up a Limited Data Set; and (b) in all other cases subject to the requirements of 45 C.F.R. §164.502(b), to the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request.

c. Obligations of Business Associate. Business Associate agrees (i) not to use or disclose PHI other than as permitted by this Agreement; (ii) to use appropriate administrative, physical, and technical safeguards and measures, including such measures required by the Security Rule, to reasonably protect the confidentiality and integrity of PHI, and to prevent use or disclosure of PHI other than as permitted by this Agreement; (iii) to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement; (iv) to report to Practice any use or disclosure of PHI not authorized by this Agreement; (v) to ensure that any agent, including a subcontractor, to whom Business Associate provides PHI agrees to the same restrictions and conditions that apply to Business Associate under this Agreement with respect to such PHI; (vi) at Practice's request, to permit Practice or an Individual to have access to PHI in a Designated Record Set in the reasonable time and manner designated by Practice; (vii) at Practice's direction, to make any amendment(s) to PHI in a Designated Record Set in the reasonable time and manner designated by Practice; (viii) to make its internal practices, books, and records relating to the use and disclosure of PHI available to Practice, or at the request of Practice to the Secretary of HHS, in a time and manner designated by Practice or the Secretary, for purposes of determining Practice's compliance with the Privacy Rule; (ix) to provide to Practice an accounting of PHI disclosures made by Business Associate, including disclosures made for treatment, payment, and health care operations, within a reasonable amount of time upon receipt of a request from Practice; and (x) to observe any limitations on disclosure of PHI of which Business Associate is timely advised pursuant to Section 4 of this Agreement.

Further, Business Associate agrees to notify Physician of any use or disclosure of PHI by Business Associate not permitted by this Agreement, any Security Incident (as defined in 45 C.F.R. § 164.304) involving Electronic PHI, and any Breach of Unsecured Protected Health Information without unreasonable delay, but in no case more than thirty (30) days following discovery of breach.

(A) Business Associate shall provide the following information in such notice to Physician: (i) the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such Breach; (ii) a description of the nature of the Breach including the types of Unsecured PHI that were involved, the date of the Breach and the date of discovery; (iii) a description of the type of Unsecured PHI acquired, accessed, used or disclosed in the Breach; (iv) the identity of the person who made and who received (if known) the unauthorized acquisition, access, use or disclosure; (v) a description of the steps taken and being taken by Business Associate to mitigate the damages and protect against future breaches; and (vi) any other details necessary for Physician to assess risk of harm to Individual(s), including steps affected Individuals should take to protect themselves.

(B) Physician will be responsible for providing notification to Individuals whose Unsecured PHI has been disclosed, as well as the Secretary and the media, as required by the HITECH Act.

(C) Business Associate agrees to establish procedures to investigate the Breach, mitigate losses, and protect against any future Breaches, and to provide a description of those procedures and the

specific findings of the investigation to Physician in the time and manner reasonably requested by Physician.

(D) The Parties agree that this section satisfies any notice requirements of Business Associate to Physician of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which no additional notice to Physician shall be required. For purposes of this Agreement, "**Unsuccessful Security Incidents"** include activity such as pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of Electronic PHI.

d. Obligations of Practice. To the extent such matters may affect Business Associate's use or disclosure of PHI, Practice shall notify Business Associate of (i) any provisions contained in Practice's notice of privacy practices produced in accordance with 45 CFR § 164.520 that are more restrictive than the practices permitted under the Privacy Rule; (ii) any changes in, or revocation of, permission by an Individual to use or disclose PHI; and (iii) any restriction upon the use or disclosure of PHI that Practice has agreed to in accordance with 45 CFR § 164.522; provided, however, that Practice's failure to provide any such notice to Business Associate in any instance shall not relieve Business Associate of its obligations to otherwise perform this Agreement or excuse any unrelated breach or non-performance hereof by Business Associate.

e. Uses and Disclosures Required by Practice. Without limiting the uses and disclosures permitted by paragraphs (iii) and (iv) of Section 2, Practice shall not request or require Business Associate to use or disclose PHI pursuant to the Agreement in any manner that would not be permissible under the Privacy Rule or the HITECH Act if done by Practice.

f. Additional Termination Rights. Practice may terminate this Agreement as to either Business Associate upon thirty (30) days prior written notice of a material breach of Business Associate's obligations under this Agreement, provided that Business Associate has not undertaken material steps to cure such breach within such 30 day period.

g. Obligations Upon Termination. Upon termination of the Agreement for any reason, Business Associate shall return or destroy all PHI received from Practice, or created or received by Business Associate on behalf of Practice, without retaining copies thereof. This provision also shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. In the event Business Associate reasonably believes that such return or destruction is infeasible, in whole or in part, Business Associate shall so notify Practice, and Business Associate instead shall comply with Privacy Rule requirements imposed on Practice in the manner stated in the next sentence. Specifically, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI in accordance with its standard data retention and destruction policies. Business Associate's obligations under this subsection (g) shall survive the termination of the Agreement.

h. Interpretation. Any ambiguity of this Agreement shall be resolved to permit the Parties to comply with the HITECH Act, HIPAA, and the Privacy and Security Rules and other implementing regulations and guidance.

i. Amendment. The parties agree to amend this Agreement at any future date as required to conform this Agreement to changes in applicable law.

In Witness Whereof the parties have caused this Agreement to be executed by their duly authorized representatives, effective _____.

Name of Practice:

_____

By: _____

Name _____

Title _____

Date_____

Ann & Robert H. Lurie Children's Hospital of Chicago, **Division of Physician Services**	**Children's Community Physicians Association**
By: _____	**By: _____**
John Salay **Director, Physician Services**	**Kena Norris** **Executive Director, CCPA**
Date:_____	**Date: _____**