

MEMORANDUM OF UNDERSTANDING

This is an agreement between the state of North Dakota acting through its Department of Health (“State”), and the _____ (“Provider”). Each of the State and _____ is sometimes referred in this Agreement as “Party” and both are sometimes referred in this Agreement together as “Parties.”

Whereas, the North Dakota Department of Health has established and maintains a statewide registry of immunization data, the North Dakota Immunization Information System (“NDIIS”) pursuant to N.D.C.C. § 23-01-05.3;

Whereas, the North Dakota Department of Health contracts with Blue Cross Blue Shield of North Dakota to maintain NDIIS;

Whereas, health care providers are required to submit immunization data to NDIIS;

Whereas, NDIIS data is Protected Health Information subject to protection under the HIPAA Rules, as amended;

Whereas, NDIIS data is accessed and disclosed in a manner consistent with state law and the HIPAA Rules;

Whereas, the North Dakota Department of Health has engaged with Blue Cross and Blue Shield of North Dakota and immunization providers to create bi-directional interoperability between the provider electronic medical record and NDIIS;

Whereas, the Provider has agreed to connect the Provider electronic health record system to NDIIS, whether directly or through third party software, and will be provided with a single security credential allowing bi-directional access to the test and production systems and databases. During the project testing phase of work, this access will allow project team members to connect and test interoperability with the NDIIS. Post project, the single security credential will allow bi-directional access to the production system and database for use by approved provider practice employees and access to the test system and database for ongoing maintenance, support, and testing;

Whereas, the parties agree to comply with the terms and conditions of this Agreement and to comply with the storage, use and disclosure of Protected Health Information under the HIPAA Rules, all as amended from time to time;

Now therefore, in consideration of the mutual promises set forth in this Agreement, the Parties agree as follows.

SECTION 1. DEFINITIONS

Catch-all definitions:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Business Associate, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Protected Health Information (“PHI”), Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

- a. Authorized User. “Authorized User” means an individual who is authorized by a Provider to access, use or disclose Protected Health Information in NDIIS and includes health care practitioners, employees, contractors, agents, or business associates of a Provider.
- b. HIPAA Rules. “HIPAA Rules” means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164.
- c. Provider. “Provider” means the means any person who delivers, administers, or supervises health care products or services, for profit or otherwise, in the ordinary course of business or professional practice and includes its Authorized Users.

SECTION 2. OBLIGATIONS AND ACTIVITIES OF PROVIDER

Provider agrees to:

- a. not use or further disclose NDIIS data other than as permitted or required by this Agreement or as required by law;
- b. require all Authorized Users to sign a confidentiality agreement before access to NDIIS is granted by the Provider. The confidentiality agreement must include the following:
 - i. statement of permitted use of data;
 - ii. statement of prohibited use and disclosure of data;
 - iii. agreement to comply with Provider’s policies, procedures, and HIPAA Rules;
 - iv. agreement to maintain NDIIS information confidential;
 - v. agreement to comply with security provisions and password protections; and
 - vi. sanctions or consequences of non-compliance.
- c. use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic PHI, to prevent use or disclosure of the PHI other than as provided for by this Agreement;
- d. comply with any limitation on the use or disclosure of a specified individual’s PHI, if the State has notified the Provider of the limitation;
- e. mitigate, to the extent practicable, any harmful effect that is known to the Provider or of a use or disclosure of PHI by the Provider or its Authorized Users in violation of the requirements of this Agreement;
- f. in accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that Business Associates and their subcontractors that create, receive, maintain, or transmit PHI received from NDIIS on behalf of the Provider agree to the same

restrictions, conditions, and requirements that apply to the Provider with respect to that information;

- g. report to State any use or disclosure of the PHI not provided for by this Agreement of which the Provider becomes aware without unreasonable delay and in any case within 30 days from the date Provider becomes aware of any such unauthorized use or disclosure, including breaches of Unsecured PHI as required at 45 C.F.R. § 164.410, and any security incident of which Provider becomes aware;
- h. in the event of a the discovery of a Breach of Unsecured PHI, Provider shall provide the State with a written notification that complies with 45 C.F.R. § 164.410 which shall include the following information:
 - i. to the extent possible, the identification of each individual whose Unsecured PHI has been, or is reasonably believed by the Provider to have been, accessed, acquired or disclosed during the breach;
 - ii. the date of discovery of the breach and date of the breach;
 - iii. the nature of the PHI that was involved;
 - iv. identity of any person who received the non-permitted PHI;
 - v. any steps individuals should take to protect themselves from potential harm resulting from the breach;
 - vi. a brief description of what the Provider is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
 - vii. any other available information that a Provider is required to include in notification to an individual under 45 C.F.R. § 164.404(c) at the time of the notification to the State required by this subsection or promptly thereafter as information becomes available.
- i. with respect to any use or disclosure of Unsecured PHI not permitted by the Privacy Rules that is caused by the Provider's failure to comply with one or more of its obligations under this Agreement, Provider agrees to pay its reasonable share of cost-based fees associated with activities State must undertake to meet its notification obligations under the HIPAA Rules and any other security breach notification laws;
- j. make any amendment(s) to PHI in a designated record set as directed or agreed to by the State pursuant to 45 C.F.R. § 164.526, or take other measures as necessary to satisfy the State's obligations under 45 C.F.R. § 164.526 within thirty (30) days after receiving a written request from the State;
- k. make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules;
- l. maintain and make available the information required to provide an accounting of disclosures to the State, within thirty (30) days after receiving a written request from

State, as necessary to permit the State to satisfy its obligations under 45 C.F.R. § 164.528;

- m. without unreasonable delay, report to State any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system of which the Provider becomes aware of in accordance with 45 C.F.R. § 164.314(a)(2)(C); and
- n. monitor and conduct audits of access to and use of NDIIIS by its authorized users.

SECTION 3. PERMITTED USES AND DISCLOSURES BY PROVIDER

a. Regulatory Duties

Provider acknowledges that it has a duty to comply with the HIPAA Rules and further acknowledges that its failure to comply with any applicable HIPAA Rules could result in civil or criminal penalties under 42 U.S.C. §§ 1320d-5 and 1320d-6.

b. General Use and Disclosure Provisions.

1. Except as otherwise limited in this Agreement, Provider may use or disclose PHI to perform its functions, activities, or services, as or as required by law.
2. Provider agrees to make uses, disclosures and requests for PHI consistent with the minimum necessary amount of information needed to perform the activities permitted in this agreement.
3. Provider may not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by the State or a Covered Entity, except that unless otherwise limited in this Agreement.
4. Except as otherwise limited in this Agreement, Provider may disclose PHI to a Business Associate for the proper management and administration of the Provider, provided the disclosure is required by law or Business Associate complies with the applicable requirements of the HIPAA Rules.
5. Provider may use PHI to report violations of law to appropriate federal and state authorities, consistent with 45 C.F.R. § 164.502(j)(1).
6. Provider may not receive direct or indirect remuneration in exchange for PHI except as permitted by the HIPAA Rules.

SECTION 4. OBLIGATIONS OF STATE

The State shall:

- a. notify Provider of any changes in, or revocation of, permission by an Individual to use or disclose his or her PHI, to the extent that any such changes may affect Provider's use or disclosure of PHI;

- b. notify Provider of any restriction on the use or disclosure of PHI that State has agreed to or is required to abide by under 45 C.F.R. § 164.522, to the extent that the restriction may affect Provider's use or disclosure of PHI.
- c. obtain any consent or authorization that may be required by applicable federal or state laws and regulations prior to furnishing PHI to the Provider; and
- d. not request Provider to use or disclose PHI in any manner that would not be permissible under the HIPAA Rules if done by State, except that the Provider may use or disclose PHI for data aggregation or management and administration and legal responsibilities of the Provider.

SECTION 5. TERM AND TERMINATION

- a. Term. The Term of this Agreement shall be effective upon execution, and shall terminate upon a thirty (30) day written notice of termination by either Party. Upon termination, all PHI provided by State to the Provider or received by Provider to the State, shall either be destroyed, returned to State or, if it is not feasible to return or destroy the PHI, protections are extended to such information, in accordance with the termination provisions in this section.
- b. Termination for Cause. Upon the non-breaching Party's knowledge of a material breach by the other Party (the "breaching party"), the non-breaching party shall either:
 - 1. provide an opportunity for the breaching party to cure the breach or end the violation within thirty (30) days and terminate this Agreement if the non-breaching party does not cure the breach or end the violation within the thirty (30) day period;
 - 2. immediately terminate this Agreement if the breaching party has breached a material term of this Agreement and cure is not possible; or
 - 3. if neither termination nor cure is feasible, report the violation to the Secretary.
- c. Obligations of Provider upon termination. Upon termination of this Agreement for any reason, Provider, with respect to PHI received from State, or created, maintained, or received by the Provider to the State, shall:
 - 1. retain only that PHI which is necessary for Provider to continue its proper management and administration or to carry out its legal responsibilities; and
 - a. continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as the Provider retains the PHI;
 - b. not use or disclose PHI retained by Provider other than for the purposes for which the PHI was retained and subject to the same conditions set out in this Agreement; and

- 2. return to the State or, if agreed to by the State, destroy the remaining PHI that the Provider maintains in any form; or
- 3. return to the State or, if agreed to by the State, destroy the PHI retained by any contractor or subcontractor when it is no longer needed for its proper management and administration or to carry out its legal responsibilities.
- d. Survival. The obligations of the Provider under this Section shall survive the termination of this Agreement.

SECTION 7. MISCELLANEOUS

- a. Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as may be amended.
- b. Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.
- c. Indemnification. Provider shall indemnify, defend, and hold State and its employees, directors, trustees, officers, representatives and agents (collectively the Indemnitees) harmless from and against all claims, causes of action, liabilities, judgments, fines, assessments, penalties, damages, awards or other expenses, of any kind or nature whatsoever, including, without limitation, attorneys’ fees, expert witness fees, and costs of investigation, litigation or dispute resolution, incurred by the Indemnitees and relating to or arising out of any material breach of the terms of this Agreement by Provider.
- d. Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

The parties have caused this Agreement to be executed on the date signed below.

PROVIDER: _____

BY: _____

ITS: _____

DATE: _____

**STATE OF NORTH DAKOTA, acting through its
Department of Health**

BY: _____

ITS: _____

DATE: _____