

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (“BAA”) is entered into by and between Trinity Health, Catholic Health East, and all of their affiliated and/or controlled healthcare organizations, including Our Lady of Lourdes Health Care Services, Inc. (“Covered Entity”) and _____ (“Business Associate”) and applies to all services provided to or on behalf of the Covered Entity and relationships between Covered Entity and Business Associate.

A. HIPAA and HITECH Dominance. In the event of a conflict or inconsistency between the terms of any other agreement between the parties and this language, this BAA language controls with respect to the subject matter herein. This language is required by the Health Insurance Portability and Accountability Act of 1996, and the Health Information Technology for Economic and Clinical Health Act (found in Title XIII of the American Recovery and Reinvestment Act of 2009) (“HIPAA” and “HITECH”). The parties acknowledge and agree that, beginning with the effective dates under HIPAA and HITECH, Business Associate will comply with its obligations under this BAA and with all obligations of a business associate under HIPAA, HITECH and any implementing regulations, as they exist at the time this BAA is executed and as they are amended from time to time, for so long as this BAA is in place. (Collectively, HIPAA and HITECH are referred to herein as “HIPAA”). The terms used in this BAA have the same meaning as defined by HIPAA unless the context dictates otherwise.

B. HIPAA Applicability and Scope; Business Associate and Subcontractors. For purposes of the obligations under this BAA, the term “Subcontractor” means, collectively, all of the Business Associate’s subcontractors as well as each of their downstream entities. Business Associate and its Subcontractors are directly subject to and must independently comply with the Business Associate provisions of HIPAA irrespective of the provisions contained in this BAA.

C. Protected Health Information. Any Protected Health Information (“PHI”) as defined by HIPAA that, on behalf of Covered Entity, was collected, created, received, maintained by or transmitted to or from Covered Entity is PHI. For purposes of these obligations PHI means all PHI in Business Associate’s possession or under its control (e.g., employees, workforce members, subcontractors and their downstream entities, and Subcontractors) and all PHI collected, created, received, maintained or transmitted by Business Associate or its Subcontractors on or after the effective date of this HIPAA language.

D. Confidential Information. Confidential Information means and includes (a) any and all information related to patients; (b) any and all information about Covered Entity that is not known to the general public; (c) non-public information that belongs or relates to third parties to whom Covered Entity has an obligation of confidentiality, including software vendors; and (d) non-public information about Covered Entity’s employees or business associates.

E. Employees, Subcontractors and Disciplinary Action

1. Acts / Omissions. Business Associate will be responsible for all actions and/or omissions by its employees and/or Subcontractor’s employees and is liable to third parties and Covered Entity for any violation of patients’ privacy or security by any person granted access or receive data through Business Associate. For purposes of this BAA, the Business Associate’s employees include its workforce members.

2. Employees. Business Associate agrees to instruct its employees regarding the confidentiality, privacy and security of PHI and the Business Associate’s obligations under this BAA. Business Associate shall not disclose to its employees or permit them to access, view,

obtain, copy, review or use any PHI that is not necessary to their services to Covered Entity. Business Associate agrees to maintain strict performance standards, including disciplinary actions, with respect to wrongful access to, copying, viewing, misuse or disclosure of PHI.

3. Workforce Members and Downstream Entities. Business Associate shall ensure its permitted workforce member(s) and Subcontractor(s) (if subcontractors are permitted) that collect, create, receive, maintain, or transmit PHI on behalf of the Covered Entity are advised in writing of Business Associate's obligations with respect to PHI. Business Associate shall require that the permitted Subcontractor(s) agree in writing to the same permissible uses and disclosures of PHI and to the same restrictions, conditions and obligations that apply to the Business Associate. Business Associate agrees to make a list of such Subcontractors available to Covered Entity upon request.

4. Administrative and Disciplinary Action. Business Associate will take appropriate administrative and disciplinary action with respect to its employee or Subcontractor if a privacy and/or security violation is substantiated.

F. Permissible Uses of PHI.

1. Using and Disclosing PHI. Business Associate is a person or an organization, other than a member of a Covered Entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a Covered Entity that involves the use or disclosure of PHI. The Business Associate may use or disclose PHI as permitted by this BAA or as required by law.

Furthermore, the Business Associate may only use or disclose PHI to the extent that the Covered Entity is permitted to use and disclose PHI and, only if, the Covered Entity has delegated that use or disclosure to the Business Associate.

2. Business Associate's Internal Management Uses of PHI. Business Associate may use PHI for internal management and administration of Business Associate, but only in connection with the direct performance by Business Associate through its employees of services for Covered Entity pursuant to this BAA.

3. Minimum Necessary. Business Associate is permitted to access, use, request and/or store only the minimum necessary PHI to the extent required to perform its duties under this BAA.

4. Handling PHI. Business Associate agrees to promptly return or destroy any PHI that is erroneously shared or delivered to Business Associate.

5. Data Aggregation. Business Associate is permitted to use PHI for data aggregation for the health care operations of Covered Entity and only as required by a written contract between Business Associate and Covered Entity or upon written request of Covered Entity. Data aggregation means combining Covered Entity's PHI with another unrelated covered entity's PHI for any purpose.

6. De-Identified – Business Associate Use for Own Purposes. Business Associate agrees not to sell (i.e., receive any direct or indirect remuneration) or use any PHI, de-identified PHI or data that identifies the Covered Entity for its own purposes or for the benefit of its other customers, without Covered Entity's prior written consent. Furthermore, in cases where the Business Associate requests consent to de-identify PHI, the Business Associate shall specify to the Covered Entity the manner in which the Business Associate will de-identify the information.

7. No Indirect Sale of PHI. Business Associate has not given Covered Entity a discount or reduction in pricing in exchange for purposes other than services to or on behalf of Covered Entity.

G. Safeguards, Reporting, and Mitigation

1. Safeguards and Security. Business Associate agrees to implement reasonable administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of all PHI. Business Associate agrees to implement reasonable electronic security practices for Covered Entity PHI which is transmitted, stored, collected, created, received, maintained or used in electronic form. Business Associate also shall require its permitted Subcontractor(s) to agree in writing to implement reasonable administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of all Covered Entity's PHI. Business Associate agrees to secure PHI through the use of encryption and/or destruction as required by Covered Entity's procedure for its internal information systems, including on portable devices and removable media. The Business Associate agrees to encrypt PHI transmitted by the Business Associate to the Covered Entity over a public network.

2. Reporting of Actual or Suspected Violations. Business Associate will report, in writing, within five (5) business days to the Covered Entity's Privacy Official and/or Security Official any actual or suspected privacy incident, breach of security, intrusion or unauthorized use or disclosure of PHI or ePHI not permitted by this BAA, made by its employees and/or Subcontractors, and will cooperate with Covered Entity in the investigation of these incidents.

Furthermore, upon request of the Covered Entity, Business Associate will report, in summary form, any unsuccessful security incident of which Business Associate becomes aware. If the definition of "Security Incident" in the HIPAA regulation is modified to remove the requirement for reporting "unsuccessful" security incidents, this paragraph shall no longer apply as of the effective date of such regulation modification.

3. Content – Reporting of Actual or Suspected Violations. The Business Associate shall report to the Covered Entity, to the best extent reasonably possible, the identification of each individual whose PHI or ePHI has been, or is reasonably believed by the Business Associate, to have been accessed, acquired, or disclosed in connection with an actual or suspected breach of privacy, security or HITECH. Business Associate shall also provide Covered Entity with any other available information that Covered Entity is required to include in a notification to an individual.

4. Mitigation. Business Associate agrees to cooperate and collaborate with the Covered Entity in mitigating any harmful effect that is known to Business Associate, including known to its employees/ Subcontractors, of a use or disclosure of PHI by Business Associate in violation of the requirements of this BAA. Business Associate also agrees to be responsible for any mitigation or compliance costs related to a breach of privacy or security caused by the Business Associate or its Subcontractors.

H. Confidentiality and Pattern of Activity.

1. Confidentiality. All Covered Entity's Confidential Information is subject to the confidentiality and use and disclosure provisions of federal and state law. Business Associate

agrees to maintain the confidentiality of, and to use or disclose, all Confidential Information in accordance with such laws.

2. **Notice of Legal Contact.** Business Associate shall promptly notify Covered Entity in writing of a disclosure request prior to disclosing Covered Entity PHI if such disclosure is required by law or court order, to the extent as permitted by law.

3. **Pattern of Activity.** If Business Associate becomes aware of a pattern of activity or practice by Covered Entity that constitutes a material breach or violation of the Covered Entity's obligations under this BAA, Business Associate will notify Covered Entity of the same.

I. **Patient Rights With Respect To PHI.** Upon request, the Business Associate shall make PHI in its possession or under its control available to the Covered Entity within five (5) business days of a Covered Entity's request.

1. **Notice of Patient Contact.** Business Associate shall promptly notify the privacy officer of Covered Entity if a patient contacts Business Associate in connection with the patient's PHI.

2. Covered Entity shall be responsible for communicating with patients regarding their patient rights.

3. **Covered Entity's Obligations.** To the extent that the Covered Entity has any limitations and/or restrictions that affect the Business Associate's use or disclosure of PHI, the Covered Entity shall so notify the Business Associate of such limitations and/or restrictions, and Business Associate shall comply with the same, including, but not limited to, those limitations listed on the Covered Entity's Notice of Privacy Practices and/or restrictions agreed upon or required by HIPAA for a specific patient.

4. If the Business Associate is engaged to maintain PHI in a designated record set, then the Business Associate agrees to honor patient rights under HIPAA.

5. Business Associate will make PHI available in electronic format upon request by Covered Entity.

6. **Electronic Health Records Related to Treatment, Payment, or Operations.** In the case of a direct request for an accounting from an individual to Business Associate related to treatment, payment or health care operations disclosures from electronic health records, Business Associate shall, in collaboration with the Covered Entity, provide such accounting to the individual in accordance with the applicable effective date of Section 13405(c) of HITECH. Business Associate shall document such disclosures and provide Covered Entity notice of the disclosure.

J. **Amendment.** Upon enactment of any law, regulation, court decision or relevant government publication and/or interpretive policy affecting the use or disclosure of PHI, Covered Entity, by written notice to Business Associate, may amend or replace this BAA in such manner as Covered Entity determines necessary to comply with same.

K. **Access for Audit.** Business Associate shall make its internal practices, books and records relating to the use and disclosure of any PHI available to Covered Entity and to other authorized government investigators for purposes of determining Business Associate's and Covered Entity's compliance with HIPAA. Business Associate agrees that Covered Entity has the right to audit, investigate, monitor,

access, review and report on Business Associate's use of any Covered Entity's PHI, with or without advance notice from Covered Entity.

L. Assignment. Business Associate may not assign any rights, nor may it delegate its duties, under this BAA without the express written consent of Covered Entity.

M. Laws. Business Associate will comply with all applicable federal and state security and privacy laws that are more protective of individual privacy and security than HIPAA.

N. Injunctive Relief. Business Associate acknowledges and stipulates that any unauthorized use or disclosure of PHI by Business Associate or any of its Subcontractors while performing services pursuant to this BAA may cause irreparable harm to Covered Entity for which Covered Entity will be entitled, if it so elects to seek injunctive or other equitable relief.

O. Termination of Relationship.

1. Immediate Termination and Cure. Covered Entity may immediately terminate its relationship with Business Associate upon written notice to Business Associate without damages, liability or penalty to Business Associate if Covered Entity determines that Business Associate has violated a material requirement related to HIPAA. Covered Entity, at its option and within its sole discretion, has the right to take reasonable steps to cure the breach and/or may (a) allow Business Associate to take steps to cure the breach, and (b) in the event of such a cure, elect to keep the this BAA and relationship in full force and effect.

2. PHI Obligations upon Termination or Expiration. Unless Business Associate is required by law to maintain PHI, Business Associate shall return or destroy (and not retain any copies of) all PHI in its possession or under its control within 30 days after the termination/expiration of this BAA. Business Associate shall seek and obtain written instructions from the Covered Entity regarding whether to return or destroy the PHI. If Business Associate is unable to return PHI and if requested to destroy the PHI and destruction is not feasible, then Business Associate shall notify Covered Entity of the reasons for being unable to return or destroy PHI in writing and must extend the protections of this BAA to the PHI and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible. Business Associate shall not transfer possession, custody or control of Covered Entity's PHI to any other person or entity without prior written approval of Covered Entity. If at any time Business Associate determines it is unable to protect the Covered Entity's PHI in accordance with the terms of this BAA, Business Associate shall destroy all Covered Entity PHI and all copies thereof and promptly provide proof of such destruction to Covered Entity.

3. Covered Entity may terminate this BAA effective immediately, if (i) Business Associate is named as a defendant in a criminal proceeding for a violation of HIPAA or other security or privacy laws or (ii) there is a finding or stipulation that Business Associate has violated any standard or requirement of HIPAA or other security or privacy laws in any administrative or civil proceeding in which Business Associate is involved.

4. Termination of Other Agreements. If this BAA is terminated for any reason, Covered Entity may terminate any or all other agreements between the parties which involve the use or disclosure of PHI. This provision shall supersede any termination provision to the contrary which may be set forth in any other agreement.

P. Prohibition of Offshore Disclosure. Nothing in this BAA shall permit the Business Associate to access, store, share, maintain, transmit or use or disclose PHI in any form via any medium with any entity or person, including the Business Associate's employees and Subcontractors, beyond the boundaries and jurisdiction of the United States without express written authorization from Covered Entity.

Q. Information System Access. This paragraph only applies in cases where the Business Associates' employees and/or its Subcontractors' employees will be provided within continuous log-on access to the Covered Entity's Information System:

1. Policies and Procedures. Business Associate agrees to comply with all of the Covered Entity's Information Systems (network, systems or applications) policies and procedures applicable to accessing, using or connecting to any Covered Entity Information System.

In cases where the Business Associate has log-on access to Covered Entity's Information Systems, including Nexus, the policies and procedures are posted and available on the Trinity Health's Nexus site. Otherwise, the Covered Entity will provide its Information System policies and procedures in advance to the Business Associate.

2. Security Codes and Passwords. Business Associate agrees that its employees will only use their access security codes or passwords to perform their duties under this BAA and that employees are strictly prohibited from disclosing their security codes or passwords to anyone, including family, friends, fellow workers (other than the system security administrator), supervisors, and subordinates for any reason. Business Associate agrees its employees will keep their security codes and passwords in confidence and not misuse or attempt to alter Covered Entity's Information System in any way.

3. Use of Access. Business Associate agrees to use its access to Covered Entity's Information Systems and Confidential Information only for treatment, payment and operations purposes permitted by HIPAA for Covered Entity's patients or to perform services for Covered Entity. Business Associate will access, use or disclose patient or business information obtained using access to the Information Systems only for the legitimate health care purposes of the Business Associate or to perform services for Covered Entity, and will only use or disclose the minimum necessary amount of information needed for the purposes identified.

4. Training. Business Associate will provide training to its employees and Subcontractors on their responsibilities for proper use of Covered Entity's Confidential Information and Information Systems. Upon request, Covered Entity will make available to Business Associate its educational brochure, "Information Privacy and Security: Your Responsibilities", in an effort to assist Business Associate in training its employees' and its permitted Subcontractors' compliance with respect to its obligations under this BAA.

5. Confidentiality Agreement for Individuals. Business Associate will require each of Business Associate's employees and Subcontractors with continuous log-on access to Covered Entity's Confidential Information and Information Systems to sign and return the Covered Entity's "Confidentiality Agreement" prior to being given continuous log-on access to the Information Systems (e.g., login ID and password).

6. Annual Review, Suspension and Termination of Access.

- i. Business Associate will cooperate with Covered Entity in the timely suspension or termination of access of any of its employees and/or Subcontractors who no longer need access to Covered Entity's Information System to carry out his/her job functions. Business Associate will complete an annual review of all employees and Subcontractors of Business Associate in an effort to identify individuals who no longer need such access.
- ii. Business Associate will immediately suspend or terminate its employee's and/or Subcontractor's access to Covered Entity's Information Systems and/or connection to a Covered Entity Network in the event of a suspected or actual violation of this BAA, and will not reinstate access and/or connection privileges until Covered Entity has agreed in writing to the reinstatement of these privileges.
- iii. Business Associate acknowledges that Covered Entity has, at its sole discretion, the right to immediately terminate any of the Business Associate's employees and/or Subcontractors right to access to any aspect of Covered Entity's Information Systems and/or Network connection in the event of Business Associate's improper use of Covered Entity's Information System and/or Network connection, Business Associate's failure to maintain the confidentiality of Covered Entity business information or any PHI, failure to maintain patient privacy or failure to safeguard and protect the security of the Information Systems and/or Network connection, or Covered Entity's PHI or business information.

7. Additional Obligations for Entities Permitted to Have Administrative Authority (Gatekeeper). In instances where the Business Associate is permitted to have administrative authority by Covered Entity to approve or revoke access to Covered Entity's Information Systems, the Business Associate agrees that it will only grant access to persons eligible under Covered Entity's policies and will not approve and request access to Covered Entity's Information Systems for individuals other than its own employees, temporary staff members, credentialed physicians and students without the prior written approval of Covered Entity. Access by all other Subcontractors requires prior written approval of Covered Entity.

R. Network Connection. This paragraph only applies in cases where the Business Associate is permitted to access Covered Entity Confidential Information via a network connection (the "Covered Entity Network"), the following provisions apply:

1. Personal Benefit. Business Associate shall not at any time or in any manner, either directly or indirectly, use for the personal benefit of Business Associate, distribute, sell, market or commercialize Covered Entity Confidential Information, create derivative products or applications based on Covered Entity Confidential Information or otherwise use Covered Entity Confidential Information in any manner not expressly permitted by this BAA.

2. Permitted Purposes of Connection. Business Associate will use or disclose PHI obtained from the Covered Entity Network only for the legitimate health care purposes of

- i. Treatment, payment and operations of the Business Associate,
- ii. To perform services for Covered Entity related to treatment, payment and operations, and/or

iii. To perform services for a health care provider that shares patients with the Covered Entity related to treatment, payment and operations of that provider.

S. Survival. The respective rights and obligations of the parties under this BAA, including without limitation the obligations of the Business Associate under Section Termination of Relationship, shall survive termination of the BAA to the extent necessary to fulfill their purposes.

COVERED ENTITY

Signature: _____

Name: _____

Title: _____

Date: _____

BUSINESS ASSOCIATE

Signature: _____

Name: _____

Title: _____

Date: _____

Email: _____

Company Name

Street Address (Suite # if any)

City, State, Zip Code

Please send a copy of the fully executed agreement to:

Trinity Health
Legal Department
20555 Victor Parkway
Livonia, MI 48152