MEMORANDUM OF UNDERSTANDING

Between:

City of Milwaukee Fire Department – Mobile Integrated Healthcare Program

And

UnitedHealthcare of Wisconsin Inc.

This Memorandum of Understanding (this "MOU"), effective as of October ___, 2016 (the "Effective Date") is between the UnitedHealthcare of Wisconsin, Inc., doing business as UnitedHealthcare Community Plan ("United"), and the City of Milwaukee Fire Department ("MFD"), in connection with its Mobile Integrated Healthcare Program ("MIH Program") (collectively, "MFD-MIH"). In this MOU United and MFD-MIH may be referred to as a "party" and collectively as the "parties."

PURPOSE:

This MOU sets forth the terms and conditions under which certain United members will participate in the MFD-MIH.

MFD OBLIGATIONS:

1. Services. MFD-MIH agrees to:

- Attempt to locate, enroll and engage United members into the MIH Program.
- Invoice United a total program cost not to exceed $1,800.00 per member without the approval of United.
- Meet monthly (at minimum) with United to review cases and determine potential next steps.
- Provide United with a Patient Outcomes Report for each member engaged in the MIH Program.

2. Subcontractors. MFD shall obtain United's written pre-approval before entering into subcontracts related to its operation of the MIH Program. United may, at any time in its sole discretion, require that subcontractors assigned to perform services in connection with the MIH Program cease providing such services. MFD is solely responsible for any payment of compensation to its subcontractors and other personnel assigned to perform services in connection with the MIH Program.

3. Protected Health Information.In connection with MFD's receipt or possession of any protected health information ("PHI") and/or personal information, MFD shall comply with the applicable provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and regulations promulgated thereunder, as may be amended from time to time, including, but not limited to the applicable privacy and security requirements of 45 C.F.R. Parts 160, 162 and Part 164, Subparts A, C and E, and the requirements set forth in Exhibit 1 to this MOU and incorporated herein. In connection with MFD's creation, receipt and storage of United member PHI, MFD shall also comply with the terms set forth in Exhibit 2 to this MOU and incorporated herein. Notwithstanding the foregoing, both parties understand and acknowledge that MFD is bound by the Wisconsin Public Records Law, Wis. Stat. sections 19.31-39 (the "Public Records Law"), and as such, the entirety of the Agreement, attachments, supporting documents, and any communications are subject to and conditioned on that law, regardless of any claim of confidentiality. MFD will notify United if a request is made for documents designated as confidential by United, MFD will allow the United the opportunity to raise and support potential exemptions under the law from public disclosure, and, if necessary, to contest the potential release of the affected records or information. United shall not make any claim against MFD if MFD makes

available to the public any document or information MFDt receives from United which is required to be made public by the MFD pursuant to the Public Records Law or a court order.

4. Compliance with Law. Contract provisions that are necessary to comply with the legal or regulatory requirements are set forth in Exhibit 3 to this MOU and incorporated herein.

UNITED OBLIGATIONS:

Services and Payment. United agrees to:

- Provide comprehensive information to the MFD-MIH on each United member that United refers to MFD to participate in the MIH Program, to facilitate MFD's outreach and MIH Program administration. United and MFD anticipate that the relay of such information shall be verbally by United case managers to MFD personnel.
- United shall pay MFD $600.00 per member to locate and engage United members to be enrolled in the MIH Program. Such amount shall not to exceed $600.00 without approval from United.
- In addition, United shall pay MFD $1200.00 per member for each United member that participates in the MIH Program.
- United shall meet monthly (at minimum) with MFD to review cases and determine potential next steps.
- During the term of this MOU and thereafter as specificed below, United will obtain and maintain, at its sole cost and expense, the insurance in the types and minimum amounts outlined below or as required by applicable law, whichever is greater, and any such additional insurance necessary to insure against claims that may arise from or in connection with its obligations under this MOU, whether such obligations are performed by MFD or a subcontractor:

  [United to provide coverage information for review by our insurance advisor]

-

OTHER OBLIGATIONS:

1. Compliance with Laws. MFD and United agree to comply with all applicable federal, state and local laws in connection with the performance of their obligations under this Agreement. MFD shall use commercially reasonable efforts to ensure all agents, employees, assigns and subcontractors that are involved in providing services in connection with the MIH Program also comply with all applicable laws.

2. Term and Termination. The term of this MOU shall commence on the Effective Date and shall remain in effect for an initial term of one year, unless other terminated in accordance with this Section. Thereafter, this MOU mayl renew for three successive one-year terms with the written consent of both parties, unless otherwise terminated under this Section. This agreement may be terminated as follows: (i) by mutual written agreement of the parties; (ii) by either party with or without cause upon at least 30 days' notice; (iii) a material breach of any provisions of MOU by either party (the "Breaching Party") shall entitle the other party (the "Non-breaching Party") to give notice of the breach to the Breaching Party specifying the nature of the breach and requiring the Breaching Party to cure such breach within 30 days, and if the breach is not cured with that 30 day period, the Non-breaching Party may terminate this MOU by delivering a second notice to the Breaching Party, specifying the termination date; (iv) by either party, immediately upon written notice to the other party in the event either party becomes insolvent or is adjudicated as a bankrupt entity, or its business comes into possession or control, even temporarily, of any trustee in bankruptcy, or a receiver is appointed for it, or it makes a general assignment for the benefit of its creditors, unless the other party elects in writing to forego termination of this MOU. Upon notice of termination of this MOU given by one party to the other, United shall pay all fees owed to MFD for

services in connection with the MIH Program performed through the effective date of termination, and MFD shall continue to provide such services until the effective date of the termination.

4. In connection with this MOU, MFD and United may need to exchange confidential and proprietary information. As a consequence, the parties agree to abide by the terms and conditions contained in Exhibit 4 to this MOU and incorporated herein, as it relates to the exchange of Confidential Information (as defined therein) between the parties.

5. MFD shall maintain, and shall require any subcontractors to maintain, books and records that are usual and customary for the provision of the MIH Program under this MOU. All such books and records shall be maintained in accordance with prudent standards of health care industry recordkeeping and all applicable laws and regulations. MFD shall preserve such records for at least ten (10) years after the date the records were created or such other period as required by applicable laws or regulation, whichever is longer. Upon reasonable notice, during normal business hours and at a reasonable time and place, United reserves the right to examine records of MFFD that directly pertain to the operation of the MHI Program for United members under this MOU. United agrees not to disrupt MFD's normal course of business while it or its designees conduct the examination, and will limit such examinations to once per annum; provider, however, that United may conduct more request examinations if it has good faith justification for doing so related to MFD's performance under this MOU.

6. Each party ("Indemnitor") will be solely financially responsible for, and will defend and indemnify the other party ("Indemnitee") from and against all claims, legal or equitable causes of action, suits, litigation, proceedings (including regulatory or administrative proceedings), grievances, complaints, demands, charges, investigations, audits, arbitrations, mediation or other process for settling disputes or disagreements, including any of the foregoing processes or procedures in which injunctive or equitable relief is sought ("Claims") made by a third party against Indemnitee arising or resulting from, or to the extent attributable to, Indemnitor's material breach of this agreement or its negligence or intentional misconduct (including fraud), except to the extent the liability results from Indemnitee's negligence, willful misconduct or breach of this agreement (including the Business Associate Agreement attached as Exhibit D hereto). Indemnitor will pay promptly and satisfy fully in connection with an indemnified Claim all (a) losses, damages of any kind or nature, assessments, fines, penalties, deficiencies, interest, payments, expenses, costs, debts, obligations, liabilities, liens or Judgments that are sustained, incurred or accrued; (b) judgments, writs, orders, injunctions or other orders for equitable relief, awards or decrees of or by any Governmental Authority ("Judgments"); and (c) costs, expenses and fees, including reasonable settlement costs, attorneys' fees, accounting fees and expert costs and fees incurred in connection with Claims. Indemnitee will provide prompt notice to Indemnitor upon learning of any occurrence or event that may result in an obligation of Indemnitor under this section and will consult with Indemnitor in the defense of, and any proposed settlement relating to, the occurrence or event, and no settlement shall be entered into without the consent of the Indemnitor. Indemnitee's failure to provide prompt notice will relieve Indemnitor of its obligations under this section, except to the extent that the omission results in a failure of actual notice to Indemnitor and Indemnitor suffers damages because of the failure to notify. Notwithstanding the foregoing, MFD does not waive any defenses or immunities to which it is entitled under law.

7. This MOU, which incorporates all exhibits and attachments hereto, constitutes the entire agreement between the parties in regard to its subject matter. Any amendment or modification to this MOU must be in writing and signed by both MFD and United, except that United may amend this Agreement unilaterally to comply with the requirements of state and federal authorities, and shall give written notice to MFD of such amendment and its effect date.

8. If any federal, state or local law, rule, regulation, or policy, or any interpretation there (including, without, limitation, any court order or ruling) at any time during the term of this MOU has a material and adverse effect on the ability of a party to receive the benefits it reasonably expects to obtain under this MOU or renders it illegal for a party to continue to perform under this MOU in a manner consistent with the parties' intent, then the parties to this MOU shall negotiate in good faith to amend this MOU to bring it into compliance, while at the same time preserving the economic expectations of the parties to the greatest extent possible.

9. During the term of this MOU, a party shall have the right to make public reference to the other party by name in an accurate, factual manner, as being involved with this MOU. The parties shall not otherwise use the other party's name, trademarks, or service marks without prior written consent from the other party. The parties mutually agree to provide, at a minimum, at least forty-eight (48) hours advance notice and opportunity to comment on all press release, advertisements, or other media statements and communications regarding this MOU, the services provided hereunder, or the business relationship between the parties. A party shall obtain the other party's written consent prior to any publication or use of such materials or communications. Nothing herein shall be construed to create a right or license to make copies of any copyrighted materials.

10. Governing Law. This MOU shall be governed by and in accordance with the laws of the State of Wisconsin, without giving effect to the conflicts of law principles thereof. The sole jurisdiction and venue for actions arising out of, or related to, this MOU shall be in the state and federal courts in Wisconsin.

11. Public Records Law Compliance. Both parties understand that the City is bound by the Wisconsin Public Records Law, and as such, all of the terms of this Agreement are subject to and conditioned on the provisions of Wis. Stat. § 19.21, et seq. Contractor acknowledges that it is obligated to assist the City in retaining and producing records that are subject to Wisconsin Public Records Law, and that the failure to do so shall constitute a material breach of this Agreement, and that the Contractor must defend and hold the City harmless from liability under that law. Except as otherwise authorized, those records shall be maintained for a period of seven years after receipt of final payment under this Agreement/

12. Notices. All notices, requests, consents, demands or other communications under this agreement will be in writing and deemed to have been duly given either (a) when delivered, if delivered by hand, sent by United States registered or certified mail (return receipt requested), delivered personally by commercial courier or (b) on the second following business day, if sent by United States Express Mail or a nationally recognized commercial overnight courier; and in each case to the parties at the following addresses (or at other addresses as specified by a notice) with applicable postage or delivery charges prepaid.

If to United:

Copy to:

If to MFD:

Attn:

13. Subcontractors. No affiliates or subcontractors to shall be used by United to perform services under this MOU without the prior written consent of MFD; and such subcontractors shall be subject to the same insurance requirements as imposed on United under this MOU, and United will be responsible for the Services to the same extent that Administrator would have been had it performed those services without the use of an affiliate or subcontractor.

14. Conflicts of Interest. No officer, employee, agent, member of the governing body, or other public official of MFD who exercises any functions or responsibilities in connection with the carrying out of any services or

requirements to which this Agreement pertains, shall have any personal interest, direct or indirect, in this Agreement. United covenants that no such person who presently exercises any functions or responsibilities in connection with this Agreement has any personal financial interests, direct or indirect, in this Agreement. United further covenants that it presently has no interest, and shall not acquire any interest, direct or indirect, which would conflict in any manner or degree with the performance of its services hereunder. United further covenants that in the performance of this Agreement, no person having any conflicting interest shall be employed. Any such interest on the part of United or its employees must be disclosed to MFD

15. Discrimination Prohibited

Administrator agrees not to discriminate against any qualified employee or qualified applicant for employment because of sex, race, religion, color, national origin or ancestry, age, disability, lawful source of income, marital status, sexual orientation, gender identity or expression, past or present membership in the military service, familial status, or based upon affiliation with, or perceived affiliation with, any of these protected categories. This requirement shall apply to, but not be limited to: employment, upgrading, demotion, transfer, recruitment, recruitment advertising, lay-off, termination, rates of pay, other forms of compensation and selection for training. Administrator shall include or cause to be included in each subcontract covering any of the services to be performed under this Agreement a provision similar to this paragraph, together with a clause requiring insertion in further subcontracts that may in turn be made.

16. Relationship of the Parties; Third Party Beneficiaries. The sole relationship between the parties is that of independent contractors. This agreement will not create a joint venture, partnership, agency, employment or other relationship between the parties. Nothing in this agreement will be construed to create any rights or obligations except among the parties; no person or entity will be regarded as a third party beneficiary of this agreement.

17. Survival. Any term of this MOU that contemplates performance after termination of this agreement will survive expiration or termination and continue until fully satisfied.

The undersigned, by signing below, acknowledges that he/she is the authorized representative for their respective Participating Agency.

AGREED TO BY:

MILWAUKEE FIRE DEPARTMENT	UNITEDHEALTHCARE OF WISCONSIN, INC.
_____	_____
Mark A. Rohlfing Fire Chief Milwaukee Fire Department	_____
_____	_____
Date	Date

EXHIBIT 1

HIPAA and GLBA
(BUSINESS ASSOCIATE AGREEMENT)

The parties hereby agree as follows:

1. DEFINITIONS

1.1 All capitalized terms used in this Exhibit not otherwise defined in this Exhibit have the meanings established in either the Agreement or for purposes of the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, as amended and supplemented by HITECH, as each is amended from time to time (collectively, "HIPAA"). To the extent a term is defined in both the Agreement and in this Exhibit or in HIPAA, the definition in this Exhibit or in HIPAA, shall govern.

1.2 "Affiliate" shall have the meaning ascribed to it in the Agreement. If the term "Affiliate" is not defined in the Agreement, then "Affiliate" shall mean, for purposes of this Exhibit, any subsidiary of UnitedHealth Group Inc.

1.3 "Breach" means the acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule that compromises the security or privacy of the PHI as defined, and subject to the exclusions set forth, in 45 C.F.R. § 164.402.

1.4 "Breach Rule" means the federal breach regulations, as amended from time to time, issued pursuant to HIPAA and codified at 45 C.F.R. Part 164 (Subpart D).

1.5 "Compliance Date" means the later of September 23, 2013 or the effective date of the Agreement.

1.6 "Electronic Protected Health Information" or "ePHI" means PHI that is transmitted or maintained in Electronic Media.

1.7 "HITECH" means Subtitle D of the Health Information Technology for Economic and Clinical Health Act provisions of the American Recovery and Reinvestment Act of 2009, 42 U.S.C. §§ 17921-17954, and all associated existing and future implementing regulations, when and as each is effective.

1.8 "PHI" means Protected Health Information, as defined in 45 C.F.R. § 160.103, and is limited to the Protected Health Information received from, or received, maintained, created or transmitted on behalf of, United (for itself and/or applicable Covered Entity customers) by Vendor in performance of the Services.

1.9 "Privacy Rule" means the federal privacy regulations, as amended from time to time, issued pursuant to HIPAA and codified at 45 C.F.R. Parts 160 and 164 (Subparts A & E).

1.10 "Security Rule" means the federal security regulations, as amended from time to time, issued pursuant to HIPAA and codified at 45 C.F.R. Parts 160 and 164 (Subparts A & C).

1.11 "Services" as used in this Exhibit, means, to the extent and only to the extent they involve the receipt, creation, maintenance, transmission, use or disclosure of PHI, the services provided by Vendor to United as set forth in the Agreement.

1.12 "Vendor" means MFD.

2. RESPONSIBILITIES OF VENDOR

With regard to its use and/or disclosure of PHI, Vendor agrees to:

2.1 not use and/or further disclose PHI except as necessary to provide the Services, as permitted or required by this Exhibit, and in compliance with each applicable requirement of 45 C.F.R. § 164.504(e), or as otherwise Required by Law; provided that, to the extent Vendor is to carry out a Covered Entity's

obligations under the Privacy Rule, Vendor will comply with the requirements of the Privacy Rule that apply to that Covered Entity in the performance of those obligations.

2.2 implement and use appropriate administrative, physical and technical safeguards and, as of the Compliance Date, comply with applicable Security Rule requirements with respect to ePHI, to prevent use or disclosure of PHI other than as provided for by this Exhibit, including at a minimum, but in any event not limited to, any safeguards set forth in the Agreement or other applicable contracts or agreements between the parties. For the avoidance of doubt, the requirements set forth in the Agreement or other applicable contracts or agreements between the parties do not limit in any way whatsoever Vendor's obligations under this Section 2.2 to comply with applicable Security Rule requirements.

2.3 without unreasonable delay, and in any event on or before 48 hours after its discovery by Vendor, report to United in writing: (i) any use or disclosure of PHI not provided for by this Exhibit of which it becomes aware in accordance with 45 C.F.R. § 164.504(e)(2)(ii)(C); and/or (ii) any Security Incident of which Vendor becomes aware in accordance with 45 C.F.R. § 164.314(a)(2)(i)(C).

2.4 without unreasonable delay, and in any event on or before 48 hours after its Discovery by Vendor, notify United of any incident that involves an unauthorized acquisition, access, use or disclosure of PHI, even if Vendor believes the incident will not rise to the level of a Breach. The notification shall include, to the extent possible, and shall be supplemented on an ongoing basis with: (i) the identification of all individuals whose Unsecured PHI was or is believed to have been involved; (ii) all other information required for or requested by United (or the applicable Covered Entity) to perform a risk assessment in accordance with 45 C.F.R. § 164.402 with respect to the incident to determine whether a Breach of Unsecured PHI occurred; and (iii) all other information reasonably necessary to provide notice to the applicable Covered Entities individuals, HHS and/or the media, all in accordance with the Breach Rule. Notwithstanding the foregoing, in United's sole discretion and in accordance with its directions, and without limiting in any way any other remedy available to United at law, equity or contract, including but not limited to any rights or remedies the United may have under the Agreement, Vendor (i) shall conduct, or pay the costs of conducting, an investigation of any incident required to be reported under this Section 2.4, (ii) shall reimburse and pay United for all expenses and costs incurred by United that arise from an investigation of any incident required to be reported under this Section 2.4 and (iii) shall provide, and/or pay the costs of providing, the required notices as set forth in this Section 2.4.

2.5 in accordance with 45 C.F.R. § 164.502(e)(1)(ii) and 45 C.F.R. § 164.308(b)(2), ensure that any subcontractors of Vendor that create, receive, maintain or transmit PHI on behalf of Vendor agree, in writing, to the same restrictions and conditions on the use and/or disclosure of PHI that apply to Vendor with respect to that PHI, including complying with the applicable Security Rule requirements with respect to ePHI; provided that, in any event Vendor shall require its subcontractors (and shall require those subcontractors to require their subcontractors) to report to Vendor any use or disclosure of PHI or Security Incident required to be reported under Sections 2.3 and 2.4 on or before 48 hours after its discovery by any of those subcontractors.

2.6 make available its internal practices, books and records relating to the use and disclosure of PHI to the Secretary for purposes of determining the applicable Covered Entity's compliance with the Privacy Rule.

2.7 document, and within 30 days after receiving a written request from United, make available to United information necessary for United or its applicable Covered Entity customer to make an accounting of disclosures of PHI about an Individual or, when and as requested by United, make that information available directly to an Individual, all in accordance with 45 C.F.R. § 164.528 and, as of the later of the date compliance is required by final regulations or the effective date of the Agreement, 42 U.S.C. § 17935(c).

2.8 provide access to United, within 15 days after receiving a written request from United, to PHI in a Designated Record Set about an Individual, or when and as requested by United, provide that access directly to an Individual, all in accordance with the requirements of 45 C.F.R. § 164.524, including as of

the Compliance Date, providing or sending a copy to a designated third party and providing or sending a copy in electronic format in accordance with 45 C.F.R. § 164.524.

2.9 to the extent that the PHI in Vendor's possession constitutes a Designated Record Set, make available, within 30 days after a written request by United, PHI for amendment and incorporate any amendments to the PHI as requested by United, all in accordance with 45 C.F.R. § 164.526.

2.10 accommodate reasonable requests for confidential communications in accordance with 45 C.F.R. § 164.522(b), as requested by United or as directed by the Individual to whom the PHI relates.

2.11 notify United in writing within three days after Vendor's receipt directly from an Individual of any request for an accounting of disclosures, access to or amendment of PHI or for confidential communications as contemplated in Sections 2.7-2.10.

2.12 request, use and/or disclose only the minimum amount of PHI necessary to accomplish the purpose of the request, use or disclosure; provided, that Vendor shall comply with 45 C.F.R. §§ 164.502(b) and 164.514(d) as of the Compliance Date.

2.13 not directly or indirectly receive remuneration in exchange for any PHI as prohibited by 45 C.F.R. § 164.502(a)(5)(ii) as of the Compliance Date.

2.14 not make or cause to be made any communication about a product or service that is prohibited by 45 C.F.R. §§ 164.501 and 164.508(a)(3) as of the Compliance Date.

2.15 not make or cause to be made any written fundraising communication that is prohibited by 45 C.F.R. § 164.514(f) as of the Compliance Date.

2.16 mitigate, to the extent practicable, any harmful effect that is known to Vendor of a use or disclosure of PHI by Vendor that is not permitted by the requirements of this Exhibit.

2.17 comply with all applicable federal, state and local laws and regulations.

2.18 not use, transfer, transmit or otherwise send or make available, any PHI outside of the geographic confines of the United States of America without United's advance written consent.

2.19 Government Program Requirements. To the extent that Vendor receives, uses or discloses PHI pertaining to Individuals enrolled in managed care plans through which United or one or more of its affiliates participate in government funded health care programs, receipt, use and disclosure of the PHI pertaining to those individuals shall comply with the applicable program requirements.

2.20 Privacy and Safeguards for NPI. Vendor understands and acknowledges that to the extent it is a nonaffiliated third party under GLBA that creates or receives NPI from or on behalf of United or an Affiliate, Vendor and its authorized representatives: (i) shall not use or disclose NPI for any purpose other than to perform its obligations under the Agreement; (ii) shall implement appropriate administrative, technical, and physical safeguards designed to ensure the security and confidentiality of the NPI, protect against any anticipated threats or hazards to the security or integrity of the NPI and protect against unauthorized access to or use of the NPI that could result in substantial harm or inconvenience to any consumer; and (iii) shall, for as long as Vendor has NPI, provide and maintain appropriate safeguards for the NPI in compliance with this Exhibit and the GLBA.

3. OTHER PERMITTED USES AND DISCLOSURES OF PHI

Unless otherwise limited in this Exhibit, in addition to any other uses and/or disclosures permitted or required by this Exhibit, Vendor may:

3.1 use and disclose PHI, if necessary, for proper management and administration of Vendor or to carry out the legal responsibilities of Vendor, provided that the disclosures are Required by Law or any

third party to which Vendor discloses PHI for those purposes provides written assurances in advance that: (i) the information will be held confidentially and used or further disclosed only for the purpose for which it was disclosed to the third party or as Required by Law; and (ii) the third party promptly will notify Vendor of any instances of which it becomes aware in which the confidentiality of the information has been breached.

4. TERMINATION AND COOPERATION

4.1 Termination. If United knows of a pattern or practice of Vendor that constitutes a material breach or violation of this Exhibit then United may provide written notice of the breach or violation to Vendor and Vendor must cure the breach or end the violation on or before 30 days after receipt of the written notice. If Vendor fails to cure the breach or end the violation within the specified timeframe, United may terminate this Exhibit and the Agreement. United also may terminate this Exhibit and the Agreement to the extent that any of United's applicable Covered Entity customers terminates its agreement with United.

4.2 Effect of Termination or Expiration. Within 30 days after the expiration or termination for any reason (or to any extent) of the Agreement and/or this Exhibit, Vendor shall return or destroy all applicable PHI, if feasible to do so, including all applicable PHI in possession of Vendor's subcontractors. To the extent return or destruction of the PHI is not feasible, Vendor shall notify United in writing of the reasons return or destruction is not feasible and, if United agrees, may retain the PHI subject to this Section 4.2. Under any circumstances, Vendor shall extend any and all protections, limitations and restrictions contained in this Exhibit to Vendor's use and/or disclosure of any applicable PHI retained after the expiration or termination (to any extent) of the Agreement and/or this Exhibit, and shall limit any further uses and/or disclosures solely to the purposes that make return or destruction of the PHI infeasible.

4.3 Cooperation. Each party shall cooperate in good faith in all respects with the other party in connection with any request by a federal or state governmental authority for additional information and documents or any governmental investigation, complaint, action or other inquiry.

5. MISCELLANEOUS

5.1 Construction of Terms. The terms of this Exhibit to the extent they are unclear, shall be construed to allow for compliance by the applicable Covered Entity and United with HIPAA.

5.2 Survival. Sections 4.2, 4.3, 5.1, 5.2, and 5.3 shall survive the expiration or termination for any reason of the Agreement and/or of this Exhibit.

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

EXHIBIT 2

SECURITY

The requirements of this Exhibit are applicable if and to the extent that: (1) Vendor accesses United Information Systems (as defined below); or (2) Vendor creates, has access to, or receives from or on behalf of United any United Information (as defined below) in electronic format. The requirements set forth in this Exhibit are in addition to, and do not substitute for, (i) any of Vendor's other obligations under the Agreement, including any Exhibits or applicable Statements of Work; and (ii) any requirements imposed upon Vendor by applicable law. To the extent that any requirements set forth in this Exhibit conflict with other requirements under the Agreement (including any Exhibits or applicable Statements of Work), then the requirement most protective of United, in United's reasonable determination, shall apply.

1. Definitions. The following terms shall have the meanings as set forth below:

1.1 "Confidential Information" has the meaning set forth in the Agreement.

1.2 "United" means UnitedHealthcare of Wisconsin, Inc.

1.3 "United Information" means any Confidential Information of United that includes or is comprised of any of the following:

(a) Protected health information (i.e., any information that would be termed "protected health information" under the provisions of the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations);

(b) Non-public personal information (i.e., any information that would be termed "non-public personal information" under the Federal Gramm-Leach-Bliley Act, any related state statutes, and any related federal or state regulations);

(c) Personal data (i.e., any information relating to an identified or identifiable natural person, as further defined under the European Union Directive 95/46/EC and each EU member state's implementing laws, including any regulations and codes of conduct issued under such laws);

(d) Cardholder data, as that term is defined in the most current version of Payment Card Industry (PCI) Data Security Standard; or

(e) Other personal information (i.e., other personally identifiable information about individuals, or information that can be used to identify individuals, the disclosure and/or use of which is restricted by applicable federal or state law, including social security numbers).

1.4 "United Information Systems" means information systems resources supplied or operated by United or its contractors, including without limitation, network infrastructure, computer systems, workstations, laptops, hardware, software, databases, storage media, proprietary applications, printers, and internet connectivity that are owned, controlled or administered by or on behalf of United.

1.5 "HITRUST" means the Health Information Trust Alliance.

1.6 "HITRUST CSF" means the HITRUST common security framework ("CSF") against which Vendor's security program will be assessed, validated and certified. The common security framework is comprised of a common set of information security requirements with standardized assessment and reporting processes accepted and adopted by healthcare organizations.

1.7 "HITRUST CSF Certification" means a CSF third-party validated report with certification, which certification has been issued by HITRUST based on testing performed by an independent CSF assessor and reviewed, approved and certified by HITRUST. In order to meet the requirements of this Exhibit, the scope of all assessment, review, testing, validation and certification activities under Vendor's HITRUST CSF Certification must include all Vendor Processing Resources and Vendor Processing, as well as applicable Vendor facilities used in connection with the provision of the Services.

1.8 "HITRUST CSF Self-Assessment Report" means the report issued by HITRUST upon its validation of the self-assessment conducted by Vendor using the standard methodology, requirements, and tools provided under HITRUST's CSF Assurance Program.

1.9 "HITRUST CSF Validated Report" means a CSF third-party validated report, issued by an authorized CSF assessor based on on-location testing.

1.10 "Independent Certification/Attestation" means (a) HITRUST CSF Certification, or (b) an alternative certification (e.g., SOC II or ISO27001) designed to document and measure performance against control objectives that map to applicable HITRUST CSF requirements, controls, and control specifications and/or other relevant standards ("Alternative Certification"), as approved by United pursuant to Section 3.3 and described in Attachment 2.

1.11 "Mitigate" means Vendor has deployed security controls as necessary to reduce the adverse effects of threats and reduce risk exposure to a level reasonably acceptable by United.

1.12 "Remediation" or "Remediate", as applicable, means that Vendor has completely resolved a security exposure or Security Incident, such that the vulnerability no longer poses a risk to United Information Systems or Vendor Processing Resources, as applicable.

1.13 "Security Incident" means the unauthorized access, use, disclosure, modification, or destruction of United Information or access to or interference with the operations of any United Information Systems or Vendor Processing Resources. Security Incidents are classified as follows:

(a) "High Severity" or severity 1 (severe impact) means external loss or exposure of United Information or impact to United Information Systems, causing significant impact to mission critical information technology systems including large-scale outages. Incidents or exposures classified at this level affect critical United Information Systems and will affect United's customers.

(b) "Medium Severity" or severity 2 (major impact) means internal loss or exposure of United Information or impact to United Information Systems, causing significant business interruption. Incidents or exposures classified at this level affect non-critical United Information Systems and may affect United's customers.

(c) "Low Severity" or severity 3 (moderate impact) means loss or exposure of United public information or impact to United Information Systems, causing a limited or confined business interruption. Incidents or exposures classified at this level affect United Information Systems or assets, but do not affect United's customers.

1.14 "Services" has the meaning set forth in the Agreement. If the term "Services" is not defined in the Agreement, then Services means any services or functions provided by Vendor to United under the Agreement.

1.15 "Vendor Processing" means any information collection, storage or processing performed by Vendor or its subcontractors (i) that directly or indirectly supports the Services or functions now or hereafter furnished to United, and (ii) involves the storage, processing, use or creation of, or access to, any United Information.

1.16 "Vendor Processing Resources" means information processing resources supplied or operated by Vendor, including without limitation, network infrastructure, computer systems, workstations, laptops, hardware, software, databases, storage media, printers, proprietary applications, Internet connectivity, printers and hard copies which are used, either directly or indirectly, in support of Vendor Processing.

2. General Requirements.

2.1 Security Program. Vendor shall maintain a comprehensive security program under which Vendor documents, implements and maintains the physical, administrative, and technical safeguards necessary to: (a) comply with applicable law; and (b) protect the confidentiality, integrity, availability, and security of Vendor Processing Resources and United Information. Vendor's security program shall be consistent with the requirements of this Exhibit and shall be designed to ensure compliance with the provisions of applicable law, including without limitation the Health Information Portability and

Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), the Payment Card Industry Data Security Standards (PCI DSS), and Sarbanes-Oxley (SOX).

2.2 Vendor Security Contact. Vendor shall designate an individual security representative to serve as the single point of contact for United on all security issues. Vendor's security representative shall be responsible for overseeing compliance with this Exhibit. Vendor shall maintain an up-to-date succession plan for the security representative role, and will replace the security representative within one business day should the individual serving as the security representative change roles or no longer be employed by Vendor. Vendor will provide United with the name of (and 24x7 contact information for) the security representative within five business days of the Effective Date and within one business day of identifying a new individual to serve in that role.

2.3 Policies and Procedures. Vendor shall maintain written security management policies and procedures to identify, prevent, detect, contain, and correct violations of measures taken to protect the confidentiality, integrity, availability, or security of Vendor Processing Resources and/or United Information. Such policies and procedures shall (a) assign specific data security responsibilities and accountabilities to specific individual(s); (b) include a formal risk management program which includes periodic risk assessments; and (c) provide an adequate framework of controls that safeguard Vendor Processing Resources, United Information Systems and United Information. Vendor shall provide such policies and procedures to United for review upon United's request at any time during the Term.

2.4 Subcontractors. To the extent that any Vendor subcontractor accesses United Information Systems or creates, has access to, receives from or on behalf of United any United Information in electronic format, Vendor shall enter into a written agreement with such subcontractor, which agreement shall incorporate all of the provisions of this Exhibit, *mutatis mutandis*.

2.5 IT Change and Configuration Management. In addition to any specific requirements set forth in the applicable Statement of Work, Vendor shall employ reasonable processes, consistent with industry best practices, for change management, code inspection, repeatable builds, separation of development and production environments, testing plans, and code escrow. Code inspections must include a comprehensive process to identify vulnerabilities and malicious code, including but not limited to logic-bombs, sniffers, and backdoors. In addition, Vendor shall ensure that processes are documented and implemented for vulnerability management, patching, and verification of system security controls prior to their connection to production networks.

2.6 Change Notifications. In addition to any specific requirements and subject to any specific conditions set forth in the Agreement or the applicable Statement of Work, Vendor shall provide United with at least 90 days' prior written notice of any relevant material changes to Vendor's information technology infrastructure, facilities, or resources associated with information security governance and oversight, security, network, and infrastructure operations and any key personnel responsible for ensuring a secure environment spanning Vendor, any of its subcontractors, and United.

2.7 Data Retention. Vendor shall not retain any United data following completion of the applicable Services, except to the extent (a) required by law, (b) required pursuant to Exhibit H (MARRA), or (c) expressly required by United in writing. At United's request, Vendor shall certify to United in writing that all United data has been returned or destroyed, as required under this Agreement.

3. Security Assessment and Independent Certification Requirements

3.1 Security Assessment. Prior to the Effective Date, Vendor shall have completed a security assessment conducted by United's Information Risk Management department ("Security Assessment"). United may require additional Security Assessments in connection with Statements of Work for new or additional Services. To the extent that the Security Assessment identifies any risks or deficiencies for which remediation is required, such remediation requirements (and the timeframes within which they must be successfully implemented) are set forth in Attachment 1 or the applicable Statement of Work. Vendor's failure to complete any remediation requirements set forth in Attachment 1 or the applicable Statement of Work within the required timeframe shall be deemed to be a material breach of the Agreement.

3.2 Independent Certification / Attestation – HITRUST CSF. Vendor shall have, as of the Effective Date, and shall maintain through the period described in Section 3.5, a HITRUST CSF Certification. To the extent that Vendor does not have

a HITRUST CSF Certification as of the Effective Date, or is the process of obtaining a HITRUST CSF Certification, the requirements of Section 3.3 or Section 3.4, as applicable, shall apply.

3.3 Independent Certification / Attestation – Other. Subject to United's prior written consent, which may be withheld or conditioned in United's sole discretion, Vendor may meet the requirements of this Section 3 by obtaining and maintaining an Alternative Certification. An Alternative Certification may include, for example, (a) a Certification Standards for Attestation Engagements (SSAE) No. 16 SOC 2 Type II certification of the security, availability and confidentiality trust services principles that map to the HITRUST CSF; or (b) for Vendor facilities and/or operations located outside of the United States, an ISO 27001 certification or its equivalent. To the extent that United approves the use of an Alternative Certification, the approved Alternative Certification and a description of the relevant control objectives or similar requirements shall be set forth in Attachment 2.

3.4 HITRUST CSF Implementation Requirements. To the extent that Vendor has not obtained a HITRUST CSF Certification (and United has not approved the use of an Alternative Certification), then (a) the requirements of Section 3.6 shall apply, and (b) Vendor shall (i) complete and provide to United a HITRUST CSF Self-Assessment Report, (ii) obtain and provide to United a HITRUST CSF Validated Report, and (iii) obtain and provide to United a HITRUST CSF Certification by the respective deadlines set forth in Attachment 3. Vendor's failure to meet the foregoing requirements shall be deemed to be a material breach of the Agreement. If Vendor has begun the process of obtaining a HITRUST CSF Certification before the Effective Date, then Vendor represents and warrants to United that all corrective action plans that are necessary to obtain a HITRUST CSF Validated Report and/or HITRUST CSF Certification and that have been identified to Vendor prior to the Effective Date are included in Attachment 3.

3.5 Independent Certification / Attestation Timing Requirements. To the extent that an Independent Certification/Attestation is required under this Exhibit, Vendor shall maintain such Independent Certification/Attestation (and continue to meet the applicable requirements of this Exhibit regarding such Independent Certification/Attestation) until the later of (a) the expiration or earlier termination of the Agreement, or (b) Vendor no longer maintains (including in archived or secure storage) or has access to, any United Information.

3.6 Interim Requirements. Until such time as Vendor obtains either a HITRUST CSF Certification or an Alternative Certification approved by United, the requirements of Attachment 4 shall apply.

3.7 Reporting of Findings. Vendor shall promptly (and in any event with 30 days of identification) report to United any findings and associated corrective action plans identified during a self-assessment or any third party assessment, including any assessment related to Vendor's Independent Certification / Attestation. Vendor will provide United with any further information associated with such findings, as reasonably requested by United.

4. Security Monitoring and Response

4.1 Mitigation and Remediation of Security Exposures. Vendor will Mitigate or Remediate any High Severity security exposure or finding discovered by United or Vendor within 24 hours from the time Vendor becomes aware of the exposure or finding. Vendor will Mitigate or Remediate any Medium Severity or Low Severity security exposure or finding discovered by United or Vendor within five business days from the time Vendor becomes aware of the exposure or finding. With respect to security exposures that are Mitigated (but not Remediated), Vendor must Remediate such security exposures within five business days after being Mitigated (in the case of High Severity exposures) and 15 business days after being Mitigated (in the case of Medium Severity exposures), and 90 days after being Mitigated (in the case of Low Severity exposures). If Vendor fails to Mitigate or Remediate any security exposure or finding within the required timeframe: (a) such failure shall be deemed to be a material breach of the Agreement; and (b) United may immediately terminate Vendor's access to United Information Systems and United Information without cost or penalty, and (i) Vendor shall not be relieved of its obligation to continue to provide the Services under the Agreement, except to the extent such Services are directly impacted by the termination of access, and (ii) Vendor's fees and charges shall be equitably reduced to reflect the Services that are no longer being provided (until access is restored, if such access is restored).

4.2 Incident Response. Vendor shall maintain formal processes to detect, identify, report, respond to, Mitigate, and Remediate Security Incidents in a timely manner.

4.3 Incident Notification. Vendor shall notify United in writing within 12 hours of any Security Incident(s) which result in, or which Vendor reasonably believes may result in, unauthorized access to, modification of, or disclosure of United Information, United Information Systems or other United applications. Vendor shall provide United with a written Remediation plan within 24 hours of the Security Incident.

4.4 Incident Remediation. Upon becoming aware of a Security Incident, Vendor will assign a severity level (i.e., High Severity, Medium Severity or Low Severity) based on the definitions set forth in this Exhibit. Vendor will reclassify the Severity Level of any Security Incident upon United's reasonable request. Vendor will Mitigate or Remediate any High Severity Security Incident within 24 hours from the time Vendor becomes aware of the incident. Vendor will Mitigate or Remediate any Medium Severity or Low Severity Security Incident within five business days from the time Vendor becomes aware of the incident. With respect to Security Incidents that are Mitigated (but not Remediated), Vendor must Remediate such Security Incidents within five business days after being Mitigated (in the case of High Severity incidents) and 15 business days after being Mitigated (in the case of Medium Severity incidents), and 90 days after being Mitigated (in the case of Low Severity incidents). If Vendor fails to Mitigate or Remediate any Security Incident within the required timeframe: (a) such failure shall be deemed to be a material breach of the Agreement; and (b) United may immediately terminate Vendor's access to United Information Systems and United Information without cost or penalty, and (i) Vendor shall not be relieved of its obligation to continue to provide the Services under the Agreement, except to the extent such Services are directly impacted by the termination of access, and (ii) Vendor's fees and charges shall be equitably reduced to reflect the Services that are no longer being provided (until access is restored, if such access is restored).

4.5 Site Outage. Vendor shall promptly report to United any Vendor site outages where such outage may impact United or Vendor's ability to fulfill its obligations to United.

5. Hosting, Virtualization Services, and Data Aggregation

5.1 Limits on Shared Hosting and Virtualization. Vendor shall not utilize (nor permit any subcontractor to utilize) any shared hosting or virtualized "cloud" hosting arrangements in support of United without United's prior written approval.

5.2 Co-Mingled or Aggregated Data. Vendor shall not store or aggregate (nor permit any subcontractor to store or aggregate) United Information or any Confidential Information of United (including, for example, program code, database scripts, data extracts, process flows, calculations, macros, and business logic) in a shared (co-mingled) environment, including cloud computing environments, databases, data warehouses or data analytics environment, without United's prior written approval. Vendor will obtain United's prior written approval of each United (or subcontractor) data center in which United Information is stored or processed.

5.3 Logical and Physical Segregation. Vendor shall physically and/or logically segregate United data from data of other Vendor customers.

6. Licenses; Software Development

6.1 No License Granted. Nothing in this Exhibit grants to Vendor, either expressly or by implication, any right or license to access or use for any purpose any United Information, United Information Systems, or any software in United's computing environments. This Exhibit does not transfer Vendor title of any ownership rights or rights in patents, copyrights, trademarks and trade secrets included in United Information Systems.

6.2 Software Usage. Vendor shall not attempt to copy, alter, decompile, reverse engineer, or disassemble any of the software programs contained in United Information Systems.

6.3 Software Development. If the Services include the development of software product(s), including web applications, for United, such software shall be developed and maintained in accordance with the development methodology specified by United. Such software shall satisfy the appropriate United information security policies and guidelines that are furnished by United to Vendor (which are incorporated herein by reference). Vendor shall comply with any instructions, guidelines or minimum compliance controls that are furnished by United to Vendor (which are incorporated herein by reference) to enable United to comply with SOX and/or other applicable laws and regulations. To the extent that Vendor uses internally-developed software or web applications to provide the Services, even if such items are not developed exclusively for United, then (a) Vendor shall insure that such items comply with any instructions, guidelines or minimum compliance

controls that are furnished by United to Vendor (which are incorporated herein by reference) to enable United to comply with applicable laws and regulations, and (b) Vendor will provide United with such information as is reasonably necessary for United to confirm that applicable compliance controls are in place.

7. Audit. Notwithstanding anything to the contrary in the Agreement, Vendor will provide to United, its auditors (including internal audit staff and external auditors), inspectors, regulators and other representatives as United may from time to time designate in writing, access at all reasonable times (and in the case of regulators at any time required by such regulators) to any facility or part of a facility at which either Vendor or any of its subcontractors is performing Vendor Processing or which contains Vendor Processing Resources, and to data and records relating to Vendor Processing, Vendor Processing Resources, and information security for the purpose of performing audits and inspections of Vendor and any of its subcontractors to (a) verify the integrity of United Information and examine the systems that process, store, secure, support and transmit United Information; (b) verify Vendor's and its subcontractors' compliance with the requirements of this Exhibit, and (c) review general controls and security practices and procedures. Vendor will cooperate fully with United or its designees in connection with audit functions and with regard to examinations by regulatory authorities. United's auditors and other representatives will comply with Vendor's reasonable security requirements in the performance of such audit.

8. Amendments. Notwithstanding anything to the contrary set forth in the Agreement, United may amend this Exhibit by providing 30 days prior written notice to Vendor if United reasonably determines that such amendment is necessary for United to comply with the Standards for Privacy of Individually Identifiable Health Information or the Security Standards for the Protection of Electronic Protected Health Information (both of which are set forth at 45 CFR Parts 160 and 164) or any other federal, state or local law, regulation, ordinance, or requirement relating to the confidentiality, integrity, availability, or security of United Information.

Attachment 1

Security Assessment Remediation Requirements

☐ Not applicable.

☐ Applicable. **[NOTE: IF APPLICABLE, COMPLETE THE TABLE BELOW.]**

#	Remediation Requirement	Completion Criteria	Implementation Date

(*add rows as necessary*)

Attachment 2

Alternative Certification Requirements

☐ Not applicable.

☐ Applicable. **[NOTE TO MFD: IF APPLICABLE, DESCRIBE ALTERNATIVE, I.E., NON-HITRUST CSF, CERTIFICATION HERE, INCLUDING DESCRIPTION OF RELEVANT CONTROL OBJECTIVES, ETC.]**

Attachment 3

HITRUST CSF Implementation Plan

☐ Not applicable.

☐ Applicable. **[NOTE TO MFD: IF APPLICABLE, COMPLETE THE FOLLOWING TABLE AND DESCRIBE ANY CORRECTIVE ACTION PLANS IN SECTION 2 BELOW.]**

1. Implementation Deadlines.

Requirement	Deadline
HITRUST CSF Self-Assessment Report	[90 days after the Effective Date]
HITRUST CSF Validated Report	[18 months after the Effective Date]
HITRUST CSF Certification	[24 months after the Effective Date]

2. Corrective Action Plans.

[NOTE: MFD TO DISCLOSE AND DESCRIBE HERE, IF APPLICABLE.]

Attachment 4

Interim Requirements

☐ Not applicable.

☒ Applicable. **[NOTE: THE ONLY CIRCUMSTANCE UNDER WHICH THIS ATTACHMENT IS NOT APPLICABLE IS IF MFD HAS A HITRUST CSF CERTIFICATION AT CONTRACT SIGNING OR IF THE VENDOR HAS AN ALTERNATIVE CERTIFICATION. IN THE CASE OF ALTERNATIVE CERTIFICATIONS, REVISIONS TO THIS ATTACHMENT MAY BE REQUIRED DEPENDING UPON THE SCOPE OF THE CERTIFICATION.]**

1. Definitions. The following terms shall have the meanings as set forth below:

1.1 "Device" means equipment or electronic media on which United Information is accessed, stored or processed, including without limitation storage drives or tapes, removable drives or media (to the extent permitted by United), desktop and laptop computers, tablets, and mobile devices.

1.2 "Vendor Personnel" will mean employees, contractors or agents of Vendor, or of its subcontractors, who provide Services (or any component thereof) to United.

2. Security Management (Infrastructure Protection)

Vendor shall maintain industry standard procedures to protect Vendor Processing Resources, including, at a minimum:

(a) Formal security programs (e.g., policies, standards, processes);

(b) Content aware solution (i.e., data loss prevention) to discover, monitor, and protect data during transit/at rest across network, storage, and endpoint systems;

(c) Processes for becoming aware of and maintaining security patches and fixes;

(d) Router filters, firewalls, and other mechanisms to restrict access to the Vendor Processing Resources, including without limitation, all local site networks that may be accessed via the Internet (whether or not such sites transmit information);

(e) Resources used for mobile access to United Information Systems shall be protected against attack and penetration through the use of firewalls, malware detection/prevention, and encryption; and

(f) Processes to prevent, detect, and eradicate malicious code (e.g., viruses) and to notify United of instances of malicious code detected on Vendor Processing Resources that may affect United Information or United Information Systems.

3. Risk Management

3.1 General Requirements. Vendor shall maintain appropriate safeguards and controls and exercise due diligence to protect United Information and Vendor Processing Resources against unauthorized access, use, and/or disclosure, considering all of the factors and/or requirements listed below. In the event of any conflict or inconsistency between relevant requirements, Vendor shall protect the United Information and Vendor Processing Resources in accordance with the most-stringent applicable requirement:

(a) Federal and state legal and regulatory requirements;

(b) Information technology and healthcare industry best practices (e.g., HITRUST Common Security Framework);

(c) Sensitivity of the data;

(d) Relative level and severity of risk of harm should the integrity, confidentiality, availability or security of the data be compromised, as determined by Vendor as part of an overall risk management program;

(e) United's data security requirements, as set forth in this Exhibit, the due diligence process and/or in the Agreement; and

(f) Any further information security requirements which are included in a Statement of Work or equivalent document which is attached to or relates to the Agreement.

3.2 Internal Risk Assessment. Vendor shall periodically (no less than annually) evaluate its processes and systems to ensure continued compliance with obligations imposed by law, regulation or contract with respect to the confidentiality, integrity, availability, and security of United Information and Vendor Processing Resources. Vendor shall document the results of these evaluations and any remediation activities taken in response to such evaluations, and provide a copy to United, upon United's request.

3.3 Internal Records. Vendor shall maintain mechanisms to capture, record, and examine information relevant to Security Incidents and other security-related events. In response to such events, Vendor shall take appropriate action to address and remediate identified vulnerabilities to United Information and Vendor Processing Resources, including as set forth in this Exhibit.

3.4 Vulnerability Assessment and Patch Management. Vendor shall provide United with the results of external vulnerability testing, internal infrastructure vulnerability testing, and application vulnerability testing. Vendor will perform (and, at United's request, allow United to perform) penetration tests of applicable Vendor environments, including perimeter vulnerability testing, internal infrastructure vulnerability testing, and application testing. Vendor shall also ensure that appropriate patches and security updates are applied in accordance with OEM recommendations or (subject to United's prior written approval) industry standards and best practices. Vendor shall provide process documentation and assessment results to United upon United's request.

3.5 Audit and Attestation Practices. Vendor shall provide to United, at least annually, information on its audit processes, procedures and controls, including a report on any findings and remediation efforts. If Vendor has not, as of the Effective Date, obtained a HITRUST CSF Certification or an Alternative Certification approved by United to permanently substitute for the HITRUST CSF Certification, then Vendor shall provide United an interim Alternative Certification. Vendor shall provide such Alternative Certification as of the Effective Date and annually thereafter until (a) annual basis, Vendor obtains a HITRUST CSF Certification, or (b) the Agreement expires or is terminated.

3.6 Vendor Locations. Unless previously authorized by United in writing, all work performed by Vendor related to the Agreement shall be performed from the Vendor location(s) designated in the Agreement and/or relevant Statement of Work(s).

4. Personnel Security

4.1 Access to United Information. Vendor shall require that Vendor Personnel who have, or may be expected to have, access to United Information or United Information Systems to comply with the provisions of the Agreement, including this Exhibit and any confidentiality agreement(s) or Business Associate Agreement(s) binding upon Vendor. Vendor will remain responsible for any breach of this Exhibit by Vendor Personnel.

4.2 Security Awareness. Vendor shall ensure that Vendor Personnel remain aware of industry standard security practices, and their responsibilities for protecting the United Information. Vendor shall provide information security awareness training and education to all Vendor Personnel upon hire, during the on-boarding process, and annually thereafter. Such information security awareness education and training shall address the responsibilities related to the Services provided to United. United may, at its option, review the content of, and request modifications to, the training curriculum. Vendor shall accommodate all of United's reasonable requests in this regard. Participation in such training by Vendor Personnel shall be mandatory and Vendor shall track attendance and, at United's request, provide a confirmation that all Vendor Personnel have completed such training. Vendor's information security awareness training shall include, but not be limited to:

(a) Protection against malicious software (such as viruses);

(b) Appropriate password protection and password management practices;

(c) Appropriate use of workstations and computer system accounts;

(d) HIPAA and HITECH requirements, including the Privacy Rule and Security Rule;

(e) Vendor's information security policies;

(f) Any applicable acceptable use policies;

(g) Relevant obligations set forth in the Agreement; and

(h) Procedures for reporting Security Incidents.

4.3 Sanction Policy. Vendor shall maintain a sanction policy to address violations of Vendor's internal security requirements or security requirements which are imposed on Vendor by law, regulation, or contract.

4.4 Supervision of Workforce. Vendor shall maintain processes for authorizing and supervising Vendor Personnel and for monitoring access to United Information, United Information Systems and/or Vendor Processing Resources.

5. Physical Security.

Vendor shall maintain appropriate physical security controls (including facility and environmental controls) to prevent unauthorized physical access to Vendor Processing Resources and areas in which United Information is stored or processed. Where practicable, this obligation shall include controls to physically protect hardware (e.g., lockdown devices). Vendor shall adopt and implement a written facility security plan which documents such controls and the policies and procedures through which such controls will be maintained. Vendor shall maintain appropriate records of maintenance performed on Vendor Processing Resources and on the physical control mechanisms used to secure Vendor Processing Resources. Vendor shall obtain United's prior written approval before moving storage or processing of United Information, or Vendor Personnel who have access to United Information or United Information Systems, to any location not previously authorized by United. Vendor agrees and acknowledges that any such relocation may require updates to any applicable Independent Attestation/Certification, and Vendor will not complete any such relocation until such updates have been completed.

6. Security Monitoring and Response

6.1 Incident Response. Vendor shall maintain formal processes to detect, identify, report, respond to, Mitigate, and Remediate Security Incidents in a timely manner.

6.2 Incident Notification. Vendor shall notify United in writing within 12 hours of any Security Incident(s) which result in, or which Vendor reasonably believes may result in, unauthorized access to, modification of, or disclosure of United Information, United Information Systems or other United applications. Vendor shall provide United with a written Remediation plan within 24 hours of the Security Incident.

6.3 Incident Remediation. Upon becoming aware of a Security Incident, Vendor will assign a severity level (i.e., High Severity, Medium Severity or Low Severity) based on the definitions set forth in this Exhibit. Vendor will reclassify the Severity Level of any Security Incident upon United's reasonable request. Vendor will Mitigate or Remediate any High Severity Security Incident within 24 hours from the time Vendor becomes aware of the incident. Vendor will Mitigate or Remediate any Medium Severity or Low Severity Security Incident within five business days from the time Vendor becomes aware of the incident. With respect to Security Incidents that are Mitigated (but not Remediated), Vendor must Remediate such Security Incidents within five business days after being Mitigated (in the case of High Severity incidents) and 15 business days after being Mitigated (in the case of Medium Severity incidents), and 90 days after being Mitigated (in the case of Low Severity incidents). If Vendor fails to Mitigate or Remediate any Security Incident within the required timeframe: (a) such failure shall be deemed to be a material breach of the Agreement; and (b) United may immediately terminate Vendor's access to United Information Systems and United Information without cost or penalty, and (i) Vendor shall not be relieved of its obligation to continue to provide the Services under the Agreement, except to the extent such Services are directly impacted by the termination of access, and (ii) Vendor's fees and charges shall be equitably reduced to reflect the Services that are no longer being provided (until access is restored, if such access is restored).

6.4 Site Outage. Vendor shall promptly report to United any Vendor site outages where such outage may impact United or Vendor's ability to fulfill its obligations to United.

7. Data and Communications Security

7.1 Exchange of United Information. Vendor shall utilize a method of transmitting United Information electronically that limits the unauthorized access to and/or modification of such information.

7.2 Data Retention. Vendor shall not retain any United data following completion of the applicable Services, except to the extent (a) required by law, (b) required pursuant to Exhibit G (MARRA), or (c) expressly required by United in writing. Subject to the foregoing, Vendor shall ensure that following the completion of the applicable Services, the United data used in connection with such Services is Securely Deleted in accordance with its records retention policy, which shall be developed by Vendor and reviewed by United. At United's request, Vendor shall certify to United in writing that all United data has been destroyed as required hereunder. As used herein, "Securely Deleted" (or "Securely Delete") means that (i) hard copy materials are destroyed and cannot be reconstructed (e.g., shredded); (ii) electronic files are deleted and overwritten to a level sufficient to ensure that they cannot be retrieved or reconstructed and that any United data contained in the files is rendered unreadable, unusable and indecipherable; and (iii) Devices are physically destroyed, degaussed or overwritten in accordance with NIST Special Publication 800-88. Vendor shall Securely Delete any United data provided by United but not required by Vendor for performance of the applicable Services promptly after Vendor discovers that such data is not needed, provided, however, that if such prompt deletion would require Vendor to reallocate resources and impact Vendor's ability to meet Service Level requirements or deadlines established by United, then United and Vendor will work together to establish a schedule for such deletion.

7.3 Encryption. Vendor shall ensure that all United data containing United Information whether stored (i.e., "data at rest") or that Vendor transmitted (i.e., "data in motion") over the public internet is encrypted using valid encryption processes. Full disk encryption must be implemented on any desktop or laptop computer on which United data is stored or processed. Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices. Valid encryption processes for data in motion are those which comply, as appropriate, with the more stringent of: (a) NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs, or (b) the requirements of applicable data security and/or privacy laws in the country from which the United Information originates, or (c) other which are Federal Information Processing Standards (FIPS) 140-2 validated. Vendor shall maintain such encryption for all transmissions by Vendor of United data via public networks (e.g., the Internet). Such transmissions include, but are not limited to:

(i) Sessions between web browsers and web servers;

(ii) Email containing United Information (including passwords);

(iii) Transfer of files via the Internet (e.g., FTP);

(iv) Laptop / desktop encryption;

(v) Mobile Device encryption; and

(vi) Removable storage media encryption (e.g., thumb drive, external hard drives, writable CD drives, backup tapes).

7.4 Protection of Systems, Devices and Storage Media. With respect to all Vendor systems or Devices containing United data, Vendor shall ensure all reasonable, industry-standard measures are taken to physically secure such Devices to prevent any unauthorized disclosure while in transit and while at rest. Vendor shall ensure that all Devices on which United data was stored or processed are Securely Deleted before such Devices are used for any other purpose. No Device on which United data was stored or processed may be sold, donated, discarded, or otherwise disposed of or used by any organization unless such Device has been Securely Deleted. All media on which United data is stored shall be protected against unauthorized access or modification. Vendor shall maintain reasonable and appropriate processes and mechanisms to maintain accountability and tracking of the receipt, removal and transfer of Devices, including certification of the Device being Securely Deleted.

7.5 Data Integrity. Vendor shall maintain processes to prevent unauthorized or inappropriate modification of United Information, for both data in transit and data at rest.

8. Access Control

8.1 Identification and Authentication. All access to any United Information or any Vendor Processing Resources shall be Identified and Authenticated as defined in this Section. "Identification" (or "Identify," as the context requires) refers to processes which establish the identity of the person or entity requesting access to United Information and/or Vendor Processing Resources. "Authentication" (or "Authenticate," as the context requires) refers to processes which validate the purported identity of the requestor. For access to United Information or Vendor Processing Resources, Vendor shall require Authentication by the use of an individual, unique user ID and an individual password or other appropriate Authentication technique approved by United in writing. Vendor shall obtain written approval from United prior to using digital certificates as part of Vendor's Identification or Authorization processes. Vendor shall maintain procedures to ensure the protection, integrity, and soundness of all passwords created by Vendor and/or used by Vendor in connection with the Agreement.

8.2 Account Administration. Vendor shall maintain appropriate processes for requesting, approving, and administering accounts and access privileges for Vendor Processing Resources and United Information. These processes shall be required for both United-related accounts and Vendor's internal accounts for Vendor Processing Resources, and shall include procedures for granting and revoking emergency access to Vendor Processing Resources and United Information. All access by Vendor Personnel to United Information Systems shall be subject to prior approval by United and shall follow United standard policies and procedures.

8.3 Access Control. Vendor shall maintain appropriate access control mechanisms to prevent all access to United Information and/or Vendor Processing Resources, except by (a) specified users expressly authorized by United and (b) Vendor Personnel who have a "need to access" to perform a particular function in support of Vendor Processing. The access and privileges granted shall be limited to the minimum necessary to perform the assigned functions. Vendor shall maintain processes to ensure that Vendor Personnel access to United Information is revoked no later than two business days upon termination and immediately in the case of involuntary termination. Vendor maintain processes to ensure that Vendor Personnel access to United Information is revoked no later than two business days upon termination and immediately in the case of involuntary termination. Vendor shall maintain appropriate mechanisms and processes for detecting, recording, analyzing, and resolving unauthorized attempts to access United Information or Vendor Processing Resources. If Vendor Personnel change roles or for any other reason no longer require access to United Information Systems, Vendor will notify United within three business days. In the case of involuntary termination, Vendor will notify United within 24 hours.

8.4 Personal Devices and Removable Media. Vendor shall ensure the Vendor Personnel will not be permitted to, and will not, utilize personal computing equipment for accessing United Information Systems or processing United Information. Vendor shall monitor and prevent United data from being sent via social media or personal email accounts. Vendor shall restrict access to, and the use of removable media, such as USB ports, writable optical media, portable hard drives, and other removable media. Vendor may not (and shall cause Vendor Personnel to not) use any such removable media to store or transfer United Information without United's prior written approval.

9. Network Security

Vendor shall only have access to United Information Systems authorized by United and shall use such access solely for providing Services to United. Vendor shall not attempt to access any applications, systems or data which United has not authorized Vendor to access or which Vendor does not need to access in order to perform Services for United. Vendor further agrees to access such applications, data and systems solely to the extent minimally necessary to provide Services to United. Vendor's attempt to access any applications, data or systems in violation of the terms in this Section shall be a material breach of the Agreement.

EXHIBIT 3

MASTER COMMUNITY & STATE APPENDIX

THIS MASTER COMMUNITY & STATE APPENDIX (this "Exhibit") supplements and is made part of the MOU. This Exhibit applies with respect to the provision of services Vendor provides for any United health plan Affiliate administering a Medicaid or other state-specific ("State") government funded and regulated program ("State Program"). In the event of a conflict between this Exhibit and other appendices or any provision of the MOU, the provisions of this Exhibit shall control except with regard to benefit plans outside the scope of this Exhibit or unless otherwise required by law or applicable State regulatory agency. As used in this Exhibit, the term Vendor means MFD. Vendor will comply with the following requirements to the extent applicable to Vendor's performance of services under the Agreement. Capitalized terms used but not defined in this Exhibit shall have the meaning assigned to them in the MOU or other applicable appendix.

1. Regulatory Approval and Filing. In the event United is required to file the MOU with federal, state or local governmental authorities, United shall be responsible for filing the MOU with such authorities as required by any applicable law or regulation. If following any such filing, the governmental authority requests changes to the MOU, Vendor agrees to cooperate with United in preparing the response to the governmental authority.

2. Compliance with Law and Government Contracts. Vendor and United agree to comply with all applicable federal, State, and local laws, rules, and regulations in connection with the performance of their obligations under the MOU. All tasks under the MOU also must be performed in accordance with the requirements of applicable contracts between any United and State and/or federal regulatory agencies. United will provide or otherwise communicate such requirements to Vendor. Vendor shall ensure all agents, employees, assigns and subcontractors, if any, that are involved in providing services under the MOU also comply with this Section.

3. Delegation and Oversight. In compliance with the delegation and oversight obligations imposed on United under their contracts with State and/or federal regulatory agencies, United reserves the right to revoke any functions or activities delegated to Vendor under the MOU, if in the reasonable judgment of United, Vendor's performance under the MOU does not comply with obligations under applicable government contracts. This right shall be in addition to United's termination rights under the MOU.

4. Press Release; Marketing; Advertising; Use of Name and Trademarks. Except as otherwise set forth in the MOU, Vendor shall not publicly use the name, logo, trademark, trade name, or other marks of United without United's prior written consent. The parties mutually agree to provide, at a minimum, at least 48 hours advance notice and opportunity to comment on all press releases, advertisements or other media statements and communications regarding the Agreement, the services or the business relationship between the parties. A party shall obtain the other party's written consent prior to any publication or use of such materials or communications. Nothing herein shall be construed to create a right or license to make copies of any copyrighted materials.

5. Offshoring. Unless previously authorized in writing by the appropriate United health plan Affiliate and State governing agency, if required, all work performed under the MOU shall be performed from location(s) in the 50 United States. If Vendor receives authorization pursuant to this Section 5 to offshore certain obligations under the MOU, United will provide, and Vendor shall comply with, all applicable offshoring regulations, requirements or restrictions, including any applicable security controls. The parties agree that any offshoring restrictions or requirements may be updated at any time to comply with applicable law and any other requirements.

6. Subcontracts. To the extent required by any regulatory agency governing any Medicare or Medicaid or other governmental benefit plans (or as may be set forth in an appendix) or any accrediting agency, Vendor shall provide advance notice to United and obtain United's consent prior to any subcontracting of any of its responsibilities under the MOU.

7. Regulatory Amendment. United may unilaterally amend this Exhibit to comply with applicable regulatory requirements required under law. Upon United's notification of such changes, United will provide notice to Vendor. If such regulatory amendment materially affects the position of either party or renders it illegal for a party to continue to perform under the MOU in a manner consistent with the parties' intent, then the parties shall negotiate further amendments to this Exhibit or the MOU as necessary to correct any inequities, to the greatest extent possible.

8. Effect of Termination or Expiration. Within 30 days after the expiration or termination for any reason (or to any extent) of the MOU and/or this Exhibit, Vendor shall return or destroy all applicable PHI, if feasible to do so, including all applicable PHI in possession of Vendor's agents or subcontractors. To the extent return or destruction of the PHI is not feasible, Vendor shall notify United in writing of the reasons return or destruction is not feasible and, if United agrees, may retain the PHI subject to this section. Under any circumstances, Vendor shall extend any and all protections, limitations and restrictions contained in this Exhibit to Vendor's use and/or disclosure of any applicable PHI retained after the expiration or termination (to any extent) of the MOU and/or this Exhibit, and shall limit any further uses and/or disclosures solely to the purposes that make return or destruction of the PHI infeasible.

EXHIBIT 4

CONFIDENTIALITY OBLIGATIONS

1. CONFIDENTIAL INFORMATION

1.1 Scope of Confidential Information.

As used in this Exhibit, "Confidential Information" means all information that is provided or made available to one Party (the "Receiving Party") by the other Party (the "Disclosing Party") in connection with the Purpose that concerns the Disclosing Party or its business operations. Confidential Information includes, but is not limited to: inventions, technologies; strategies; trade secrets; customer and supplier lists; product designs and pricing information; processes; formulas; business plans; provider, employer and consumer information; employee data; health plan relationships; acquisition plans; product licensing plans; budgets, finances, and financial plans; production plans and protocols; systems architecture, technology, data, and methods, and any other information that by its nature would typically be considered non-public information. The Purpose and the fact that discussions or negotiations regarding the Purpose have occurred or are occurring are also considered Confidential Information for purposes of the MOU. Confidential Information may be conveyed to the Receiving Party in written, electronic, or oral form, and includes any information that may be derived from or developed as a result of access to the Disclosing Party's facilities, as well as all notes, reports, evaluative materials, analyses or studies prepared by the Receiving Party or its directors, officers, employees, agents and advisors (collectively, such Party's "Representatives") regarding or relating to the Disclosing Party or its Confidential Information.

1.2 General Exclusions.

Notwithstanding the foregoing, the following will not constitute Confidential Information for purposes of this Exhibit:

(i) information that was already in the Receiving Party's possession before receipt from the Disclosing Party, as evidenced by written records, provided that such information was obtained lawfully and without an obligation of confidentiality to the Disclosing Party or another person or entity;

(ii) information that was obtained by the Receiving Party from a source other than the Disclosing Party, provided that such information was obtained lawfully and without an obligation of confidentiality to the Disclosing Party or another person or entity;

(iii) information that is or becomes generally available to the public, other than as a result of a disclosure by the Receiving Party;

(iv) information that was independently developed by or for the Receiving Party without reference to the Disclosing Party's Confidential Information, as evidenced by written records.

2. NONDISCLOSURE OBLIGATIONS

2.1 Protection of Confidential Information.

Each Party agrees that it will: (i) hold the Disclosing Party's Confidential Information in confidence and protect it as confidential and proprietary utilizing standards of care appropriate for the healthcare industry; (ii) disclose the Disclosing Party's Confidential Information only to its own Representatives who have a legitimate need to know such information in connection with the Purpose, and who are made aware of this Exhibit and bound by confidentiality requirements as strict as those set forth herein; and (iii) use the Disclosing Party's Confidential Information only as required in connection with the Purpose. As between the Parties, each Party will be and remain solely and completely liable and responsible for any breaches of this Exhibit committed by any of its Representatives and will immediately notify the other Party if it becomes aware of any such breaches.

2.2 Compelled Disclosure.

If the Receiving Party is requested or required by applicable law or legal process to disclose the Disclosing Party's Confidential Information, the Receiving Party will (to the extent permitted by law) provide the Disclosing Party with prompt notice of any such request or requirement and reasonably cooperate in any efforts by the Disclosing Party to seek an appropriate protective order or other remedy or otherwise challenge or narrow the scope of such request. If a protective order or other remedy is not obtained, the Receiving Party will furnish only that portion of the Confidential Information that it is advised, by written opinion of counsel, is legally required, and the Receiving Party will exercise reasonable efforts to obtain

reliable assurance that such Confidential Information will continue to be held in confidence. Disclosures of Confidential Information that are required by applicable law or legal process will not be breaches of this Exhibit.

2.3 Return of Materials.

The Receiving Party will return all copies of the Disclosing Party's Confidential Information upon the earlier of (i) the Disclosing Party's request, or (ii) the termination or expiration of the MOU. Instead of returning such Confidential Information, the Receiving Party may (if the Disclosing Party consents in writing) destroy all copies of such Confidential Information in its possession, and certify in writing to the Disclosing Party that it has done so. Unless prohibited in writing (before disclosure) by the Disclosing Party, or if required by law, the Receiving Party may retain a copy of any Confidential Information disclosed to it solely for archival purposes, provided that such copy is retained in secure storage and held in the strictest confidence for so long as the Receiving Party's obligations of confidentiality under this Exhibit continue.

3. OWNERSHIP AND TITLE; NO WARRANTY; NO FURTHER OBLIGATION

3.1 Ownership and Title.

All Confidential Information is and will remain the sole and exclusive property of the respective Disclosing Party. The Receiving Party acquires no right, title or license to the Disclosing Party's Confidential Information. Each Party acknowledges and agrees that the furnishing of its Confidential Information is not intended to and does not restrict the Receiving Party's (or any of its affiliates') ability to (i) carry on their existing business activities, (ii) enter into any new lines of business, (iii) develop or market new products or services, or (iv) otherwise expand their business operations, provided that in each case the undertaking of such activities does not otherwise violate this Exhibit.

3.2 No Warranty; No Further Obligation.

All Confidential Information disclosed hereunder is disclosed on an "AS IS" basis with no warranties, express or implied, of any kind. The Disclosing Party will have no liability relating to the use of its Confidential Information, or any errors or omissions in its Confidential Information. The Parties may rely solely on representations or warranties regarding Confidential Information that are made under the final written agreement (if any) regarding the Purpose. Nothing in this Exhibit will impose any obligation upon either Party to consummate the Purpose (or any other business transaction) or to enter into any further discussions or negotiations.

4. REMEDIES

Each Party agrees that the other Party may suffer irreparable harm and that monetary damages would not be a sufficient remedy for any breach or threatened breach of this Exhibit. Each Party therefore agrees that, in addition to any other legal or equitable remedies available, the aggrieved Party will be entitled to specific performance and injunctive or other equitable relief as a remedy for any such breach or threatened breach. Each Party further agrees to waive, and use its commercially reasonable efforts to cause its Representatives to waive, any requirement for the securing or posting of any bond in connection with such remedy and the aggrieved Party will not be required to prove damages in order to avail itself of such equitable relief.