BON SECOURS MERCY HEALTH

CUSTOMER TERMS AND CONDITIONS

These Customer Terms and Conditions ("**Customer Terms**") govern the purchase order, requisition, or other similar document (including any attachments provided in connection therewith, the "**Purchase Order**") that has been transmitted (via facsimile, e-mail or other means) to vendor identified on the Purchase Order ("**Vendor**") by Bon Secours Mercy Health, Inc. ("**BSMH**") or one of its Affiliates or facilities ("**Facilities**") identified in the Purchase Order (BSMH and Facilities collectively and individually referred to as "**Customer**"). Notwithstanding any prior dealings between Customer and Vendor, the Purchase Order is expressly made conditional on, and Customer expressly limits Vendor's provision of any Products or Services set forth in the Purchase Order to, the terms and conditions in the Agreement (as defined below).

By accepting the Purchase Order and/or starting performance, shipping any Products or furnishing any Services in connection with the Purchase Order, Vendor acknowledges that Vendor has read, understands, and agrees to be bound by the terms and conditions set forth in the Agreement. If Vendor objects to any such terms and conditions, Vendor shall (a) notify Customer in writing within three days after its receipt of the Purchase Order and (b) withhold acceptance of the Purchase Order and not start any performance, ship any Products or furnish any Services (or provide any deliverable arising therefrom) in connection with the Purchase Order until/unless such objection is settled in writing signed by Customer and Vendor.

These Customer Terms are specific to the Purchase Order and may hereafter be revised, from time to time, by Customer. Revised terms and conditions will be posted on Customer's website or attached or referenced in a Purchase Order, and if applicable, will be immediately effective for Purchase Orders issued thereafter. **Accepting such Purchase Order and/or starting performance, shipping any Products or furnishing any Services after a revised version of Customer Terms have been posted, Vendor will be deemed to have accepted the revised version.**

"Services" shall mean all consulting and professional Services, development, installation and training Services, maintenance, support, technical and help desk 24X7 support and all other Services provided under the Agreement. Services shall be performed in accordance description of Services agreed to by Customer in writing and as described in the Purchase Order. "Products" shall mean all products, supplies, Software, equipment, accessory, other tangible Products, and related documentation, specifications, and instructions for use ("**Documentation**") provided under the Agreement.

1. **ENTIRE AGREEMENTS; AMENDMENTS.**
(a) "Agreement" means (i) the Purchase Order and the signed agreement between Customer, and Vendor or its affiliate, (A) that is in effect at the time the Purchase Order is issued, (B) that contains a provision indicating that such signed agreement is the entire agreement between the parties with respect to its subject matter and (C) under which the Purchase Order is issued, based on the subject matter of the Purchase Order or a statement in the Purchase Order expressly identifying such signed agreement, or (ii) if no such signed agreement exists, then the Purchase Order and these Customer Terms. The Agreement (1) contains the entire understanding of Customer and Vendor with respect to the subject matter of the Purchase Order and incorporate all representations, warranties, covenants, commitments and understandings on which Customer and Vendor have relied, and neither party makes any other representations, warranties, covenants, commitments or understandings; and (2) supersede all previous representations, warranties, covenants, commitments and understandings between Customer and Vendor, written or oral, with respect to the subject matter of the Purchase Order.
(b) No modification, amendment or waiver of any term or condition in the Purchase Order or herein shall be effective, nor shall any additional or different terms or conditions, whether set forth in an invoice, confirmation, acceptance, shrink-wrap license, click wrap license, online terms of use or service or elsewhere, or pursuant to any course of dealing, usage of the trade or Customer's acceptance of any Products or Services, be effective, unless set forth in a writing signed by Customer and Vendor.

2. **INSPECTION, TESTING, AND REJECTION**. Payment for Products hereunder shall not constitute acceptance thereof. Customer shall have the right to inspect Products and to reject any and all Products which are in Customer's judgment defective and/or fail to perform in accordance with manufacturer specifications. Products so rejected may be returned to Vendor at Vendor's expense. In addition, at Customer's option, Vendor will promptly correct or replace the rejected Products at Vendor's expense, including transportation, freight, insurance, and handling costs, but no Products returned as defective will be replaced without Customer's written authorization. In the event Customer receives Products whose defects or nonconformity are not apparent on examination; Customer reserves the right to require replacement Products at a later date.

3. **SHIPPING.** At no time will Vendor assess Customer any transportation, freight, insurance, or handling costs associated with the provision of Products to Customer or Customer's authorized distributor. In limited circumstances, Customer may direct that Products be shipped directly to a Customer facility within twenty-four hours of the placement of a Purchase Order. In that case, Vendor shall pay all transportation, freight, and insurance expenses and add such expenses as a separate line item to the invoice.

4. **NON-CONFORMING PRODUCTS OR SERVICES; LATE DELIVERY; REPLACEMENT PERSONNEL.**
(a) Customer reserves the right to refuse any Products or Services and to cancel all or any part of the Purchase Order if Vendor does not, or Products or Services provided by Vendor to Customer do not, conform to any applicable industry standards or practices, any applicable specifications, drawings, samples, descriptions or any other similar criteria in the Purchase Order or otherwise provided to Vendor by Customer (the "**Specifications**") or any terms and conditions set forth in the Purchase Order and herein. Acceptance of any part of the shipment of Products or any part of the Services shall not bind Customer to accept any non-conforming Products or non-conforming Services simultaneously provided by Vendor, nor deprive Customer of the right to reject any previous or future non-conforming Products or Services. Customer may, if it rejects any non-conforming Products, return such Products to Vendor at Vendor's expense for transportation both ways, and Vendor shall not deliver to Customer any replacement or substitution Products for such rejected Products unless so authorized by Customer.
(b) The delivery of Products and Services shall strictly comply with the delivery date or delivery schedule, if any, provided to Vendor by Customer. If at any time it appears Vendor will not meet such delivery date or schedule, Vendor shall promptly notify Customer in writing of reasons for, and the estimated duration of, the delay. If requested by Customer, Vendor shall ship such delayed Products by means to avoid or minimize delay to the maximum extent possible, including rerouting any shipment if appropriate and the use of a dedicated motor carrier or air freight, and any added costs shall be borne by Vendor.
(c) With respect to any personnel assigned by Vendor to provide Products or Services to Customer, Customer reserves the right to request for any lawful reason whatsoever the removal or reassignment of any such personnel, which right shall not relieve Vendor of any responsibility it has for the Purchase Order. Vendor shall as soon as possible thereafter provide replacement personnel satisfactory to Customer. Vendor shall not, however, leave any position(s) without staffing acceptable to Customer during any replacement assessment period(s).(d) Notwithstanding the foregoing, Customer may cancel the Purchase Order and seek any other remedies available in accordance with applicable law, including cover and incidental and consequential damages from Vendor if Vendor does not, or Products or Services provided by Vendor to Customer do not, conform to the Purchase Order Specifications and these terms and conditions, including delivery of Products or Services that do not strictly comply with the or the delivery date or schedule, if any, provided to Vendor by Customer.

5. **CANCELLATION**. Customer may cancel the Purchase Order at any time and for any reason upon written notice to Vendor. In the event of such cancellation, Vendor shall comply with any directions given by Customer in such notice with respect to the Products and Services in the Purchase Order and cease all other shipment and delivery of Products and Services with respect to the Purchase Order. Within fifteen (15) days from the effective date of such cancellation, Vendor shall provide to Customer all material, drawings, work-in-progress and co-developed intellectual property (in the state of completion or non-completion in which they exist on the date of cancellation) and submit an invoice to Customer for all Products and Services provided by Vendor and accepted by Customer in accordance with the Purchase Order prior to cancellation, but only to the extent relating to such Products or Services for which Vendor has not already submitted an invoice to Customer. Customer agrees to pay all undisputed amounts in accordance with the Agreement. In no event shall Customer be responsible for any amounts in the aggregate greater than (a) the total that would have been due under the Purchase Order or (b) the value of the work done by Vendor in accordance with the Purchase Order prior to cancellations, whichever is less.

6. **COMPLIANCE; STANDARDS**.
a) Vendor Compliance. Vendor shall ensure that all Services and Products are provided and maintained throughout the term of the Agreement to be in compliance with: (i) the standards of the Joint Commission, to the extent applicable; (ii) all applicable Federal, State, and local laws, ordinances, codes, regulations, and rules and data protection and data breach notification obligations; and (iii) the applicable policies and procedures of Customer; all as may be amended from time to time.
b) Vendor Representations Regarding Exclusion.
   i. Vendor ensures: (A) upon hire or engagement and monthly thereafter, that none of its employees or subcontractors that provide Products or Services are listed on the Office of the Inspector General ("**OIG**") and General Services Administration's Systems for Award Management ("**SAM**") excluded persons, sanction and debarment lists, state Medicaid exclusion lists, or the Office of Foreign Asset Control ("**OFAC**") Specially Designated Nationals and Blocked Persons list; (B) Vendor shall immediately advise BSMH of any violation of this paragraph and a violation of this paragraph shall be grounds for immediate termination with cause under the Agreement; and (C) Vendor shall permit BSMH to audit and monitor Vendor activity, including, but not limited to, access to records and physical

locations for compliance to this paragraph.

ii. Vendor represents, warrants, and covenants that its ability to provide Products and Services in any state, commonwealth or other jurisdiction has not been revoked, limited, suspended or otherwise restricted in any material manner. In the event that during the term of the Agreement, Vendor is charged with a felony or Vendor's ability to provide Products and Services in any state, commonwealth or other jurisdiction is revoked or becomes limited, suspended or otherwise restricted in any material manner, Vendor shall immediately advise BSMH and such event shall be grounds for immediate termination with cause under the Agreement.

c) Access to Records. Pursuant to 42 U.S.C. § 1395x(v)(1)(I), to the extent applicable, until the expiration of four (4) years after termination of the Agreement, Vendor shall agree to make available to the Secretary of Health and Human Services, the U.S. Comptroller General, and their representatives, if requested by any of the foregoing agencies or representatives, the Agreement and all books, documents and records necessary to certify the nature and extent of the costs of those services. If Vendor carries out the duties of the Agreement through a subcontract worth $10,000 or more over a 12 month period with a related organization, the subcontract shall also contain an access clause to permit access by the Secretary, Comptroller General, and their representatives to the related organization's books and records.

d) Reporting of Discounts. Vendor agrees to properly report and disclose discounts and fees in the Agreement, to the extent required by applicable state and federal law. Vendor agrees to comply with the requirements of 42 U.S.C. §1320a-7b(b)(3)(A) and the safe harbor regulations regarding discounts or other reduction in price. Vendor shall satisfy any and all requirements imposed on sellers by the safe harbor. In accordance with 42 C.F.R. § 1001.952(h), Vendor shall (a) fully and accurately report any discount on invoices, statements, or reports submitted to Customer, or (b) where the value of a discount is not known at the time of a sale, fully and accurately report the existence of a discount program on the invoice, statement or reports submitted to Customer and when the value of the discount becomes known, provide Customer with documentation of the calculation identifying the specific Products or Services purchased to which the discount shall be applied.

e) Patient Safety; Product Recalls. In the event Products are purchased hereunder, Vendor will comply with all Customer policies and procedures and other requirements, including, but not limited to those concerning patient care, safety, and risk management. Vendor will immediately notify Customer of any Product defect or recall, or any adverse or near miss event that does or has the potential to impact patient safety. Vendor will cooperate with Customer in the investigation and mitigation of all actual or near miss events involving the Product or Services provided by Vendor including any Software or data breach issues. Vendor will cooperate with Customer in responding to or resolving any complaint, investigation, inquiry or review initiated by a governmental agency or otherwise and cooperate with any insurance company providing protection to Customer in connection with the foregoing as allowed by law. Vendor agrees to promptly replace any Product in the event the Product cannot be repaired or promptly corrected to meet all applicable health and safety standards.

f) Medicare Compliance. One or more BSMH Affiliates may be a First Tier Entity of a Medicare Advantage Organization and/or a Medicare Part D Plan Sponsor and may have agreed to ensure that organizations providing health or administrative services to it comply with the Center for Medicare and Medicaid Services ("**CMS**") updated guidance on compliance program requirements and related provisions published in Pub. 100-18, Medicare Prescription Drug Benefit Manual. Accordingly, in the event this Agreement covers such services, Vendor hereby warrants and represents that: (i) within ninety (90) days of hire or engagement, and no less than annually thereafter, its employees and subcontractors providing services will complete CMS' General Compliance Training and fraud, waste, and abuse ("**FWA**") training, through a Vendor program that meets Medicare standards or through the DHHS website (which can be accomplished at no cost to Vendor); (ii) Vendor has a Code of Conduct/Compliance Policy in place which is provided or is available for viewing to all of its employees and subcontractors providing Services within ninety (90) days of hire/contracting, annually and when changes are made; (iii) employees and subcontractors are informed of how to report any compliance concerns and suspected or actual misconduct for internal investigation including the obligation to report such instances to BSMH; (iv) Vendor ensures upon hire or engagement and monthly thereafter, that none of its employees or subcontractors that provide Services are listed on the Office of the Inspector General (OIG) and General Services Administration's Systems for Award Management (SAM) excluded persons, sanction and debarment lists; (v) Vendor ensures that a record of compliance with the above is maintained for a period of ten (10) years, and with thirty (30) days' prior written notice, will provide evidence of compliance to BSMH; (vi) Vendor maintains a non-retaliation policy; and (vii) Vendor shall permit BSMH to audit and monitor Vendor activity, including, but not limited to, access to records and physical locations.

g) Notice to Vendors; Social Imperatives; ERDS. Vendor agrees to comply with Customer's Notice to Vendors, attached as **Attachment 1**, understands the requirements set forth in that document, agrees to abide thereby and represents and warrants to BSMH that Vendor is not prohibited from doing business with BSMH under the criteria set forth in **Attachment 1**. The Customer Statements on Social Imperatives set forth in **Attachment 2** are hereby incorporated by reference and made part of this Agreement. Vendor acknowledges that Customer conducts its business in compliance with the most current published Ethical and Religious Directives for Catholic Health Care Services, promulgated by the United States Conference of Bishops ("**ERDs**").

h) Nondiscrimination in Employment. Vendor, in performing the work required by the Agreement, agrees not to discriminate against any employee or applicant for employment because of race, religion, color, gender, age, marital status, national origin, sexual orientation, gender identity, genetic information, veteran status, disability or other characteristic protected by law and to insert the provisions of this paragraph into any subcontracts issued under this Agreement.
i) Conflict of Interest. Vendor hereby represents and warrants that it does not have: (a) any relationships that could constitute a conflict of interest, or the appearance of a conflict of interest with healthcare providers on the medical staffs of the Customer hospital facilities utilizing the equipment, supplies, or services being provided under this Agreement; or (b) any contractual, ownership or financial relationship, whether direct or indirect, with any Customer employee or board member that is involved in obtaining, approving, retaining, negotiating or otherwise managing the relationship between Vendor and Customer. Furthermore, contemporaneous with the execution of this Agreement, Vendor shall disclose to BSMH, all of the relationships it has with healthcare providers on the medical staffs of the BSMH hospital facilities utilizing the equipment, supplies, or services being provided under this Agreement. Such disclosure shall be by way of a brief written description.

7. **AFFILIATE ORDERING; GPO**.
a) Affiliates. Customer Affiliates may purchase Services or Products from Vendor directly by entering into an order form with Vendor referencing this Agreement. By such Affiliate entering into an order form hereunder, the Affiliate agrees to be individually, and not joint and severally, bound by the terms of this Agreement as if it were an original party hereto and for purposes of such order form, shall also be deemed "Customer" hereunder. Unless stated otherwise on an order form, Customer or its Affiliate which signs the order form under this Agreement shall be deemed to be individually, and not jointly and severally, liable for a breach of this Agreement and Vendor shall pursue any and all remedies available under this Agreement solely and exclusively against such Affiliate. "**Affiliate**" means: (a) an entity controlling, controlled by, or under common control with a Party (an entity will be deemed to have control if it owns over 50% of another entity), (b) a joint venture or ownership interest in which a Party or its Affiliates maintain a meaningful economic interest and/or board representation, and/or (c) any entity for which Customer is responsible for providing IT or supply chain services.
b) GPO. In the event Vendor and a group purchasing organization ("**GPO**") of which Customer is a member, enters into a master agreement or pricing agreement governing the purchase and sale of any or all the Products or Services hereunder ("**GPO Agreement**"), Vendor agrees that Customer shall have the option, in Customer's sole discretion and upon prior notice to Vendor and on a prospective basis only, to (i) continue this Agreement, but to adjust the pricing hereof to reflect the pricing set forth in the GPO Agreement, without any penalty, or (ii) terminate this Agreement, without any penalty, and enter into the GPO Agreement.

8. **SOFTWARE.** If the Products set forth in the Purchase Order include any software (including pursuant to a software-as-a-service offering), related documentation and/or updates thereto (collectively, "**Software**") the following terms and conditions apply:
a) Vendor shall retain all intellectual property rights in and to the Software. Vendor hereby grants to Customer and its Affiliates a perpetual (unless otherwise limited in the Purchase Order to a specific duration), worldwide, non-exclusive license to access and use the Software for the business purposes of Customer and its affiliates. If the Purchase Order limits the Software to use by a certain number of users, then Customer may replace a user with another user from time to time, provided that the then-current number of users using the Software does not exceed such number. If Vendor determines that Customer and its affiliates have exceeded rights to the Software in the Purchase Order through increased usage that is otherwise in accordance with these terms and conditions, Vendor shall promptly notify Customer in writing of such excess usage and Customer shall thereafter promptly eliminate such excess usage. If Customer does not eliminate such excess usage, Vendor's exclusive remedy shall be to invoice Customer proportionately for such excess usage using the pricing set forth in the Purchase Order.
b) Customer and its Affiliates may (i) make a reasonable number of backup or archive copies of any Software provided by Vendor and (ii) permit one or more third parties to exercise the rights granted to Customer and its Affiliates hereunder, provided that any such third party may only use the Software to provide Products to or perform Services for Customer and its Affiliates..

9. **PAYMENT; TAXES; AUDITS.**
a) Payment. Unless otherwise instructed by Customer, Vendor shall comply with invoice instructions provided by Customer. Customer shall make payment by Electronic Funds Transfer, check, or credit card within sixty (60) days from receipt of an uncontested invoice. To the extent Vendor and Customer agree in writing that Customer will reimburse Vendor for travel expenses associated with Services to be performed pursuant to this Agreement, Vendor shall comply with Customer's travel expense policy communicated to Vendor.
b) Customer does not pay penalties or interest on late payments or any other fees, except as set forth in the Purchase Order. Pricing is fixed at the pricing set forth in the Purchase Order. Any tariffs on imports are the responsibility of Vendor and will expressly not be passed on to BSMH. Products opened but not delivered to Customer's surgery field will be replaced by Vendor at no cost to

Customer without a restocking fee. Vendor will issue to Customer full credit or replacement for any Product determined to be unusable during a surgical procedure. Customer may cancel the Purchase Order any time before Vendor ships to Customer.
c) Vendor shall invoice Customer in accordance with the Purchase Order and include on all invoices (i) the Purchase Order number; (ii) a description of Products and/or Services provided; (iii) the price set forth in the Purchase Order, including a detailed description of the number of hours worked and fee per hour, if Services are provided based on time and material pricing; and (iv) expenses and pass-through costs approved by Customer, including details around such costs. Customer shall not be obligated to pay any amounts not properly invoiced within 90 days after Products and/or Services are provided, including any pass-through expenses that otherwise would have been reimbursable in accordance with the Purchase Order. Except for amounts expressly set forth in the Purchase Order, Customer shall not be responsible for any (a) other charges, including charges for delivery, parts or services and (b) expenses of Vendor or any mark-ups on any expenses of Vendor.
d) Taxes. Vendor acknowledges and agrees that Customer is a not-for-profit entity and is exempt from paying certain taxes. Vendor shall not charge to Customer any taxes that Customer is not legally obligated to pay.
e) Audits. BSMH may conduct external invoice audits for price compliance at its own expense utilizing a third party. In the event Vendor is found to be in material non-compliance with the pricing terms of this Agreement (>5%), Vendor will: (a) reimburse BSMH for the full third-party audit expense (not to exceed $7500 per year), and (b) reimburse BSMH the total amounts overpaid by BSMH. BSMH expressly reserves the right to offset payments due to Vendor by any amounts to be reimbursed under this provision.

10. **SUBCONTRACTING**. Unless otherwise agreed by Customer in writing, which agreement shall not be unreasonably withheld, Vendor may not subcontract the performances of Vendor's obligations hereunder. In the event a subcontractor performs Vendor's obligations under this Agreement, Vendor shall be responsible and liable for any acts or omissions of such subcontractors. Vendor may utilize such staff as may be employed by or under contract with Vendor and as it deems necessary to perform the Services; provided, however, that if Vendor staff is onsite, BSMH shall have the right to request removal of any such Vendor staff if BSMH has a reasonable basis to conclude that such Vendor staff poses a threat to employee or patient safety, jeopardizes the quality of services at a BSMH facility, has violated or is likely to violate the Notice to Vendors, jeopardizes the confidentiality, integrity and/or availability of BSMH's Confidential Information (defined herein) or could otherwise damage the reputation of BSMH. Vendor hereby agrees to immediately remove any such staff upon receipt of BSMH's request made under this Section.

11. **TERM; TERMINATION.** The term of this Agreement shall begin upon execution of the Agreement by the parties and end upon the termination or expiration of the last order form or statement of work unless the parties agree otherwise. Notwithstanding anything else contained in the Agreement, Customer may terminate the Agreement, without penalty, in whole or in part at any time, without cause, upon not less than ten (10) days' prior written notice to Vendor. Vendor shall not suspend delivery of Products and/or performance of Services during the term of this Agreement for Customer's material breach of the Agreement, but Vendor may remedy any material breach by termination of the Agreement as described herein. The Agreement may be terminated by either party if the other party materially breaches any provision of the Agreement and either the breach cannot be cured or, if the breach can be cured, it is not cured by breaching party within thirty (30) days after breaching party's receipt of written notice of such breach.

12. **VENDOR ACCESS MANAGEMENT**. Vendor agrees to register with BSMH's vendor access management system prior to providing products and/or services and will be responsible for annual credentialing fees.

13. **WARRANTIES.**
a) Services Warranties. To the extent that Vendor provides Services pursuant to the Agreement, Vendor represents and warrants to Customer that it shall perform the Services using personnel of required skill, experience and qualifications and in a professional and workmanlike manner in accordance with generally recognized medical industry standards of care for similar services and shall devote adequate resources to meet its obligations under the Agreement.
b) Product Warranties. To the extent that Vendor provides Products pursuant to the Agreement, Vendor represents and warrants to Customer that such Products (i) materially conform to Documentation, (ii) shall be free from material defects in design, material and workmanship, (iii) shall be fit for their intended purpose and operate as intended; (iv) shall be delivered free and clear from all liens and encumbrances, (v) shall meet the generally recognized medical industry standards of care for similar products, and (vi) Vendor owns all rights, title, and interest in and to the Products, subject to the Software Warranty herein. Such warranty shall cover any modifications made to the Product by Vendor.
c) Third Party Warranties. To the extent Vendor provides Products manufactured by a third party vendor, Vendor shall assign and deliver to Customer all representations and warranties received by Vendor from third party vendors related to the Products and/or Services, to the extent such representations and warranties may be assigned. To the extent such third party representations

and warranties are not assignable, Vendor will enforce such against a third party on Customer's behalf.

14. CONFIDENTIALITY; DATA; PRIVACY & SECURITY.

a) Confidentiality. Vendor shall hold the Confidential Information of Customer in strict confidence and shall (i) comply with all applicable laws and regulations regarding such Customer's Confidential Information, (ii) unless required by law, shall not make Customer's Confidential Information available to any third party, (iii) except as otherwise authorized by Customer in writing, limit access to Customer's Confidential Information to those of its and its Affiliates' employees and contractors who need that access for purposes consistent with this Agreement and who have agreed in writing to follow procedures no less protective of the Confidential Information than those herein, or (iv) use Customer's Confidential Information for any purpose other than to perform its obligations under the Agreement. If Vendor is required by law or court order to disclose Customer's Confidential Information, then Vendor shall, to the extent legally permitted, provide Customer with advance written notification and cooperate in any effort to obtain confidential treatment of Customer's Confidential Information. As between the parties, Customer retains all right, title and interest (including any and all intellectual property rights) in and to Customer's Confidential Information and any modifications made thereto in the course of the operation of the Service or Product. Subject to the terms of this Agreement, Customer hereby grants to Vendor a non-exclusive, worldwide, royalty-free right to use, copy, store, transmit, modify, create derivative works of, and display the Customer Data solely to the extent necessary to provide Products and Services to Customer, or to prevent or address support or technical problems under this Agreement, or as may be required by law. "**Confidential Information**" shall mean all information, whether written, electronic or oral, whether or not marked, designated or otherwise identified as "confidential," including, without limitation, information about its business affairs, Customer Data, patients, including any Protected Health Information (as such term is defined by applicable federal or state law or regulations, including, but not limited to the Health Insurance Portability and Accountability Act of 1994, as amended ("**HIPAA**") and 42 C.F.R. Part 2 relating to substance abuse and mental health information) (collectively, "**PHI**") and any "Personally Identifiable Information" ("**PII**") (including, but not limited to, any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor to the government). Confidential Information does not include information that: (i) is in the possession or control of Vendor without restriction at the time of its disclosure hereunder; (ii) is, or becomes publicly known, through no wrongful act of Vendor; (iii) is received by Vendor from a third party free to disclose it without a confidentiality obligation, or (iv) is independently developed by Vendor and which Vendor is able to demonstrate the independent development. The Vendor may disclose Confidential Information of the Customer pursuant to the requirements imposed by a governmental agency or by operation of law applicable to Vendor, provided that such Vendor gives the Customer written notice thereof, to the extent Vendor is not prohibited by such governmental agency or law, as soon as practicable and reasonably cooperates with the Customer to contest such disclosure.

b) Customer Data. "**Customer Data**" means any data, metadata, materials, or information (regardless of form, medium, or source from which derived) provided or made available or accessible to Vendor by, or that are otherwise owned by or relate to, Customer or to any of its customers, end-users, patients, health care providers, payers, employees, agents, and representatives or created by Vendor to perform Services for Customer, including, for example: (i) any data, materials, or information at any time maintained or stored in, or created or generated by or in connection with the use or operation of, any information systems, databases, or Software of Customer (including any data in any information systems, databases, or Software maintained for or on behalf of Customer or its patients or customers); or (ii) all summaries, indexes, and aggregations of any such data, materials, and information (regardless of whether owned by Customer or any third party, or whether input, generated, produced, or compiled by Customer, by any third party suppliers or service providers of Customer, by any end- users, or by Vendor); or (iii) all other records, data, files, input materials, processed data, results of data analyses, information, reports, forms, and other items of or relating to Customer that may be received, computed, transmitted, developed, used, or stored by Vendor, or by any of Vendor's personnel, for or on behalf of Customer, in connection with this Agreement, but excluding in any event any data and information regarding the internal business operations of Vendor and any correspondence between the parties, to the extent such data, information, and correspondence do not contain items described in this clause (iii).

c) No Aggregation. Vendor shall not compile, aggregate, distribute, and/or disclose statistical analyses and reports utilizing Customer Data; provided that upon Customer's written request and direction, Vendor may compile, aggregate, and/or distribute Customer Data to Customer for the sole and exclusive purpose of preparing statistical analysis and reports for Customer. Vendor shall be prohibited from disclosing, directly or indirectly, any Customer Data, in any form, whether de-identified or not, whether compiled or aggregated with any third party, without the express written consent of Customer.

d) Equitable Relief. Customer may seek equitable relief (including injunctive relief) against Vendor and its agents to prevent the breach or threatened breach of this Confidentiality Section, in addition to all other remedies available at law, and Vendor hereby waives any requirement for the securing or posting of any bond or the showing of actual monetary damages in connection with such claim.

e) Return or Destroy Confidential Information at Termination. On termination of the Agreement and except as required by law, Vendor shall, at no additional cost, promptly return all of Customer's Confidential Information provided to it, together with all copies thereof, or destroy such Confidential Information and certify in writing that such Confidential Information has been destroyed within 30 days of the termination of the Agreement. Vendor shall accomplish the destruction of Customer's Confidential Information by "purging" or "physical destruction", in accordance with the National Institute of Standards, Guidelines for Media Sanitization, SP800-88, Appendix A - see http://csrc.nist.gov/.

f) Privacy and Security. At all times during the term of the Agreement, Vendor will comply with applicable privacy and security laws and implement and adhere to current industry practices with respect to security of Customer's Confidential Information, including, without limitation, the Information Security Guidelines attached and incorporated by reference as **Attachment 3**, to the extent applicable. In the event Vendor hosts Customer Data, then Vendor shall notify Customer of the location within the continental United States where Customer Data will be hosted. In the event Vendor hosts Customer Data through a third party, then Vendor shall notify Customer that Customer Data is hosted by a third party and the name of the third party and the location within the United States where Customer Data is hosted. Vendor is responsible and shall be liable for any breach of this Agreement related to hosting Customer Data, whether Vendor or third party hosts Customer Data.

g) HIPAA; GDPR; PCI/DSS. Vendor represents it is not a business associate as defined by HIPAA. Vendor does not require disclosure of PHI to perform its obligations under this Agreement, Vendor acknowledges and affirms it shall not collect or attempt to collect PHI from Customer. In the event that disclosure of PHI may occur or is required to perform the Services or deliver the Products to Customer under the Agreement, the parties agree to comply with a business associate agreement ("**BAA**") executed by the parties, or if the parties have not executed a BAA, then agree to comply with the business associate agreement attached hereto as **Attachment 4**. Vendor and its authorized subcontractors shall comply with applicable international laws regarding privacy and security of Customer's Confidential Information, including the General Data Protection Regulation ("**GDPR**"), and Vendor is responsible and shall be liable for any breach of the Agreement and this Section, whether such breach is by Vendor or its subcontractors. Upon request of Customer, Vendor shall execute such additional documents (e.g., a data processing agreement) as requested by Customer to remain in compliance with the GDPR or other state or federal laws (e.g., the California Consumer Protection Act). To the extent applicable, Vendor shall comply with the requirements of Payment Card Industry/Data Security Standards (PCI/DSS) – see http://www.pcisecuritystandards.org.

15. **OFFSHORE SERVICES**. Vendor and its subcontractors shall not perform Services under this Agreement outside of the United States without the express written consent of Customer. To the extent that offshore arrangements are permitted and used in this Agreement, Vendor hereby acknowledges and affirms: (a) Vendor has policies and procedures in place for offshore subcontractors to ensure that PHI and other personal information remains secure; (b) Vendor's offshore subcontracting arrangement(s) expressly prohibit offshore subcontractor's access to Customer Data not associated with Customer's third-party payor contracts; (c) Vendor has offshore subcontracts in place that allow for immediate termination of the subcontract upon discovery of a significant security breach; (d) Vendor's offshore subcontracting arrangement includes all required Medicare Part C and D language (e.g., record retention requirements, compliance with all Medicare Part C and D requirements, etc.); (e) Vendor will conduct an annual audit of each offshore subcontractor providing Services under this Agreement. The audit results will be used by Vendor to evaluate the continuation of its relationship with the offshore subcontractor; and (f) Vendor agrees to share its offshore subcontractor's audit results with Customer and Customer's third-party payers upon written request. Offshore for purposes of this Agreement is as defined by Medicare and refers to any country that is not one of the fifty United States or one of the United States Territories.

16. **PUBLICITY**. Neither party shall, without the prior written approval of the other party, engage in any publicity, advertising or marketing activities relating to the Agreement, the subject matter hereof, or the other party.

17. **INDEMNIFICATION.**

a) Customer Indemnification of Vendor. Customer will defend Vendor from and against any and all claims, causes of actions, demands, liabilities, losses, damages, deficiencies, judgments, settlements, interest, awards, penalties, fines, costs, and expenses, including reasonable attorneys' fees and witness' fees, (collectively "**Claims**") by a third party alleging failure by Customer to obtain consent to disclose Customer Data to Vendor, and will indemnify and hold harmless Vendor from and against any Claim awarded against Vendor or agreed in settlement by Customer resulting from such Claim; provided that such indemnification, defense, and hold harmless shall not extend to any matter to the extent caused by the negligence or misconduct of Vendor or its affiliates or their directors, employees, agents, successors, and assigns.

b) Vendor Indemnification of Customer. Vendor will indemnify, defend, and hold harmless, at its own expense, Customer and each of its affiliates and their directors, employees, agents, successors and assigns ("**Customer Indemnitees**") from and against any and all Claims arising from or related to the negligence, action or failure to act, or breach of any representation, warranty, covenant, or obligation of Vendor or its affiliates or their directors, employees, agents, successors, or assigns; provided that such

indemnification and hold harmless shall not extend to any matter to the extent caused by the gross negligence or intentional misconduct of Customer.

c) Intellectual Property Indemnification. Vendor will defend, at its own expense, Customer Indemnitees from and against any Claims alleging that any Products or Services infringes a patent, copyright, trademark, or any other proprietary or intellectual property right and will indemnify and hold harmless Customer Indemnitees from and against any such Claims awarded against Customer or agreed in settlement by Vendor resulting from such Claims. If Customer's use of the Products or Services are (or in Vendor's opinion are likely to be) enjoined or if Vendor determines the following actions are reasonably necessary to avoid material liability, Vendor may, in its sole discretion, either: (i) substitute substantially functionally similar products or services; (ii) procure for Customer the right to continue using the Products or Services; or (iii) if (i) and (ii) are not commercially reasonable, terminate this Agreement and refund to Customer the Fees paid by Customer for the Products or Services that were prepaid but not used by Customer.

d) Indemnification Procedures. In the event of a potential indemnity obligation under this Indemnification Section, the indemnified party will: (i) promptly notify the indemnifying party in writing of the Claim, (ii) allow the indemnifying party the right to control the investigation, defense and settlement (if applicable) of such Claim at the indemnifying party's sole cost and expense, and (iii) upon request of the indemnifying party, provide all necessary cooperation at the indemnifying party's expense. Failure by the indemnified party to notify the indemnifying party of a Claim under this Section shall not relieve the indemnifying party of its obligations under this Indemnification Section, however the indemnifying party shall not be liable for any litigation expenses that the indemnifying party incurred prior to the time when notice is given or for any damages and/or costs resulting from any material prejudice caused by the delay or failure to provide notice to the indemnifying party in accordance with this Indemnification Section. The indemnifying party may not settle any Claim in any matter that would require obligation on the part of the indemnified party (other than payment or ceasing to use infringing materials), or any admission of fault by the indemnified party, without the indemnified party's prior written consent, such consent not to be unreasonably withheld, conditioned or delayed. Further, any indemnification obligation under this Indemnification Section will not apply if the indemnified party settles or makes any admission with respect to a Claim without the indemnifying party's prior written consent. For Claims alleging violations of Federal or state statute (or implementing regulation), the indemnified party will have the option at any time either (i) to tender its defense to the indemnifying party, in which case indemnifying party will provide qualified attorneys, consultants, and other appropriate professionals to represent the indemnified party's interests at the indemnifying party's expense, or (ii) undertake its own defense, choosing the attorneys, consultants, and other appropriate professionals to represent its interests, in which case the indemnifying party will be responsible for and pay the reasonable fees and expenses of such attorneys, consultants, and other professionals. A party's failure to perform the remedies set forth in this Indemnification Section are in addition to, and not in lieu of, all other remedies that may be available to a party under this Agreement or otherwise.

18. **DAMAGES**.

a) No Indirect Damages. IN NO EVENT SHALL EITHER PARTY OR ITS AFFILIATES BE LIABLE UNDER THIS AGREEMENT TO THE OTHER PARTY OR ANY THIRD PARTY FOR CONSEQUENTIAL, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR PUNITIVE DAMAGES, ARISING OUT OF OR RELATING TO ANY BREACH OF THIS AGREEMENT, REGARDLESS OF (i) WHETHER SUCH DAMAGES WERE FORESEEABLE, (ii) WHETHER OR NOT THE OTHER PARTY WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND (iii) THE LEGAL OR EQUITABLE THEORY (CONTRACT, TORT OR OTHERWISE) UPON WHICH THE CLAIM IS BASED.

b) Exceptions. INDIRECT DAMAGES PERMISSIBLE. SUBSECTION (a) OF THIS INDIRECT DAMAGES SECTION SHALL NOT APPLY TO VENDOR'S (i) INDEMNIFICATION OBLIGATIONS, (ii) LIABILITY FOR GROSS NEGIGLENCE OR WILLFUL MISCONDUCT AND (iii) BREACH OF CONFIDENTIALITY, PRIVACY, SECURITY, AND/OR BUSINESS ASSOCIATE AGREEMENT OBLIGATIONS.

c) IN NO EVENT WILL CUSTOMER OR ITS AFFILIATES BE LIABLE FOR DAMAGES OR LOSSES THAT EXCEED, IN THE AGGREGATE, THE GREATER OF (i) THE AMOUNT DUE FROM CUSTOMER AS SET FORTH IN THE PURCHASE ORDER BUT NOT ALREADY PAID TO VENDOR FOR THE GOODS OR SERVICES PROVIDED BY VENDOR IN ACCORDANCE WITH THE PURCHASE ORDER AND THESE CUSTOMER TERMS, OR (ii) $1000. THIS SECTION WILL NOT APPLY ONLY WHEN AND TO THE EXTENT THAT APPLICABLE LAW SPECIFICALLY REQUIRES LIABILITY DESPITE THE FOREGOING DISCLAIMER, EXCLUSION AND LIMITATION.

d) IN THE EVENT ANY DOCUMENT PREPARED BY VENDOR CONTAINS A LIMITATION OF LIABILITY, SUCH LIMITATION OF LIABILITY SHALL NOT APPLY TO VENDOR'S (i) INDEMNIFICATION OBLIGATIONS, (ii) LIABILITY FOR GROSS NEGIGLENCE OR WILLFUL MISCONDUCT AND (iii) BREACH OF CONFIDENTIALITY, PRIVACY, SECURITY, AND/OR BUSINESS ASSOCIATE AGREEMENT OBLIGATIONS.

19. **INSURANCE**.

a) Minimum Limits. Vendor shall maintain, at its expense, insurance coverage for Vendor for claims made during and after termination of the Agreement based on conduct or events having occurred during the term of the Agreement, with policy limits at a minimum of the following:

i. Workers Compensation – statutory limits containing a waiver of subrogation against Customer and its affiliates, with Employer's Liability of One Million Dollars ($1,000,000) per each accident and One Million Dollars ($1,000,000) per each employee disease with a One Million Dollars ($1,000,000) policy limit;
ii. Employer's Liability – One Million Dollars ($1,000,000) per each occurrence;
iii. Commercial General Liability (CGL) – (bodily injury and property damage combined) to include Blanket Contractual coverage with combined single limit, bodily injury and property damage liability or at least One Million Dollars ($1,000,000) per each occurrence and Three Million Dollars ($3,000,000) in the annual aggregate;
iv. Business Automobile Liability insurance – One Million Dollars ($1,000,000) per combined single limit per accident for bodily injury; provided that owned, hired and non-owned automobiles are used in performance of Vendor's obligations under the Agreement and policies may not have a deductible exceeding Ten Thousand Dollars ($10,000);
v. Product Liability/Completed Operations with a Combined Single Limit coverage for Bodily Injury and Property Damage of at least Five Million Dollars ($5,000,000) per each occurrence and Ten Million Dollars ($10,000,000) in the annual aggregate;
vi. Professional Liability – One Million Dollars ($1,000,000) per each occurrence and Three Million Dollars ($3,000,000) in the annual aggregate or, to the extent that the Services are provided in a jurisdiction with statutory limitations on medical malpractice liability, then limits shall be not less than the current statutory limits per each occurrence and three times such amount in the annual aggregate; provided however, that, if the Services are of the nature that Professional Liability insurance would be customary and appropriate and Vendor does not have professional liability coverage, Vendor may substitute Errors and Omissions coverage in the amount of not less than One Million Dollars ($1,000,000) per each occurrence and Three Million ($3,000,000) in the annual aggregate; and
vii. Cyber Liability, also known as Data Breach Coverage, of at least Ten Million Dollars ($10,000,000) per each occurrence; and (viii) such other coverages as maybe required by Customer based on the nature of the Services provided (e.g., pollution, legal liability, fidelity).

b) Insurance Standards. All insurance policies required shall be issued by insurance companies licensed to do business in the relevant state or states and with a minimum A. M. Best rating of A-. With the exception of Workers' Compensation and Employers' Liability insurance, Customer shall be an additional insured on Vendor's insurance policies. All insurance certificates shall provide for at least thirty (30) days notification from insurer to Customer before coverage is canceled or materially changed. Vendor shall provide to Customer an insurance certificate indicating the foregoing coverage prior to the effective date of the Agreement. The provisions of this Section shall survive termination or expiration of the Agreement.

20. **GENERAL TERMS**.

a) Status of Parties. The parties to this Agreement are independent contractors. There is no relationship of partnership, joint venture, employment, franchise or agency created hereby between the parties.

b) Governing Law; Jurisdiction. The Agreement shall be governed by and construed in accordance with the laws of Ohio, without giving effect to its principles of conflict of laws. Any action or proceeding arising out of or related to this Agreement shall be brought only in a state or federal court of competent jurisdiction located in Hamilton County, Ohio. Each party hereby consents to the personal jurisdiction of such courts.

c) Assignment. The rights and obligations of the Agreement may not be assigned or delegated by either party without the prior written consent of the other party, except that either party may assign the Agreement to any of its Affiliates or in connection with a merger, reorganization, acquisition, transfer, or sale of all or substantially all of its assets, unless such assignment is to the competitor or other commercially reasonable objection to such assignment, in which case the non-assigning party may terminate the Agreement, without penalty.

d) Remedies. Any termination by either Party, whether for cause or otherwise, shall be without prejudice to any claims for damages or other rights against the other Party that preceded termination. No specific remedy set forth in the Agreement shall be in lieu of any other remedy to which a Party may be entitled pursuant to the Agreement or otherwise at law or equity. Nothing in this Agreement shall be construed as a waiver by either party of its ability to defend against liability, limits of liability, or of its right to assert other defenses otherwise available to it by operation of law, including but not limited to the statute of limitations. Furthermore, no provision in this Agreement shall be construed as limiting a party's right to seek remedies available to it by operation of law in circumstances involving personal injury arising in connection with the Agreement. Anything contrary

to this in the underlying Agreement is superseded by this paragraph. Furthermore, any reference to statutory provisions includes those provisions as amended and the interpretive regulations issued thereunder.

e) Severability. In the event any part or parts of the Agreement, including the Customer's Terms and any Attachments hereto, are held to be unenforceable, the remainder of the Agreement, including any Attachments, thereto will continue in effect.

f) Notices. Any notice or communication required or permitted under this Agreement will be in writing to each party at such party's address set forth in the Purchase Order to the attention of Chief Legal Officer and will be deemed to have been received by such party: (i) if given by hand, immediately upon receipt; (ii) if given by overnight courier service, the first business day following dispatch; or (iii) if given by registered or certified mail, postage prepaid and return receipt requested, the second business day after such notice is deposited in the mail.

g) Notification of Claims. Each party agrees to promptly notify the other party of any incidents, Claims, or lawsuits involving the Services or Products and provide reasonable access to records or information necessary to resolve the Claim.

h) Force Majeure. Neither Party will be liable for any failure or delay in performing an obligation under the Agreement that is due to any of the following causes, to the extent beyond its reasonable control: acts of God, accident, riots, war, terrorist act, epidemic, pandemic, quarantine, civil commotion, breakdown of communication facilities, breakdown of web host, breakdown of internet service provider, natural catastrophes, governmental acts or omissions, changes in laws or regulations, national strikes, fire, explosion, generalized lack of availability of raw materials or energy.

i) Complete Agreement. The Agreement and all attached exhibits and schedules, including the Customer's Terms and related "**Attachments**," constitute the entire understanding and agreement between Customer and Vendor relating to the subject matter hereof and supersedes all prior or contemporaneous negotiations, agreements and understandings, whether oral, written, or established by the course of dealing of the parties, , including, but not limited to, all prior agreements between Customer and Vendor.

j) Survival. The following Sections shall survive: Compliance, Payment, Vendor Representations, Publicity, Confidentiality, Customer Data, Privacy and Security, Indemnification, Limitation of Liability, Insurance, Offshore Services, Term, Termination, General Terms, and any Sections or obligations which by their nature are intended to survive, and the exhibits and schedules, including Attachments, referenced in such Sections.

ATTACHMENT 1

NOTICE TO VENDORS

Bon Secours Mercy Health, Inc. ("**BSMH**") has created a Compliance Program to ensure we comply with all laws and regulations that apply to a tax-exempt, church-based health care provider. This includes laws concerning health and safety, Medicare and Medicaid, fraud and abuse, tax, anti-trust, environmental and labor laws, among others.

We cultivate a culture of compliance from the Board Rooms to front-line caregivers, and we include our credentialed providers, and vendors in that commitment. We commit to an effective Compliance Program to sustain that culture. Our program includes education, communications methods to encourage reports of concerns, investigations into concerns, monitoring and auditing for compliance and accuracy, and accountability and corrective action when we detect an error.

Vendors must be aware of, and agree to abide by, the following provisions of our Compliance Program as a continuing condition to do business with us:

Eligibility to Do Business with a BSMH Entity

1. As a Medicare-participating organization, we are prohibited from hiring or doing business with any entity or person who has been:
    - **A.** Excluded from participating in federal or state health programs by the Office of Inspector General of the U.S. Department of Health and Human Services.
    - **B.** Barred from contracting with the U.S. Government by the General Services Administration; or
    - **C.** Listed as a Terrorist Organization or supporting individual by the Office of Foreign Asset Control of the U.S. Department of the Treasury.
2. Vendors must certify their eligibility to do business with a BSMH entity by certifying that neither the organization, nor its owners or principals or any vendor employee (collectively, "**staff**") who will provide services to the BSMH entity is prohibited from doing business with BSMH under paragraph 1. Vendor agrees abide by the BSMH Exclusion Screening Policy.
3. Eligibility is a continuing condition of any contract with BSMH, and vendors must agree to notify BSMH immediately if the government takes adverse action in paragraph 1 against Vendor or any of its staff. Vendor must also notify BSMH if they learn of an investigation that could reasonably result in adverse action in paragraph 1 against Vendor or its staff. BSMH may terminate a contract where the government takes adverse action listed in paragraph 1 against Vendor or its staff.

Business Ethics, Gifts and Gratuities

4. BSMH does business in an open, fair, impartial, and transparent manner and engages in arms-length negotiations with potential vendors. BSMH requires our employed associates, credentialed providers, board members and volunteers to always act in the best interests of BSMH. This includes avoiding conflicts of interest that might jeopardize the impartiality of their judgment and decision-making, as well as avoiding situations that create a reasonable appearance of a conflict of interest or an appearance of favoritism, partiality, personal gain, or insider-dealing.
5. BSMH associates may not seek, request, or accept any gift, gratuity or other item, regardless of value, that is intended to influence a business decision, or that is offered to them because of their position in a pending business decision. BSMH associates may not accept gifts, gratuities, discounts, or other things of value from anyone doing business with, or desiring to do business with, BSMH or any BSMH entity, except in nominal amounts, which they must disclose to their reporting superior.
6. The Compliance Program includes a Compliance Officer ("**CO**") who can assist or respond to any vendor concern about possible violations of BSMHs policies or applicable laws or regulations. Associates are required, and vendors are encouraged, to report any concerns anytime, 24/7/365, via our online webform at https://bsmh.cqs.symplr.com/Portal/CreateForm/450009 or by phone at 1-888-302-9224. BSMH policy prohibits retaliation for a report made in good faith.

Required Education on the False Claims Act and Whistleblower Protections for Providers of Medicaid-covered Services

Because BSMH and its entities receive more than Five Million Dollars ($5,000,000) in annual Medicaid reimbursements, we are required to provide additional education to our employed associates, vendors related to the False Claims Act and whistleblower protections available under those laws. Our vendors are required to ensure that their employees who will provide services to BSMH receive the following educational information also:

BSMH associates work hard to ensure that we create accurate and truthful patient bills and submit accurate claims for payment from any payer, including Medicare and Medicaid, commercial insurance, or our patients. It's the right thing to do, and federal and state laws require accuracy in health care billing.

The federal False Claims Act (31 USC 3729-33) makes it a crime for any person or organization to knowingly make a false record or file a false claim with the government for payment. "Knowing" can include deliberate or reckless ignorance of facts that make the claim false.

Examples of possible False Claims include someone knowingly billing Medicare for services that were not provided, or for services that were not ordered by a physician, or for services that were provided at sub-standard quality where the government would not pay.

A person who knows a False Claim was filed for payment can file a lawsuit in Federal Court on behalf of the government and, in some cases, receive a reward for bringing original information about a violation to the government's attention. Penalties for violating the federal False Claims Act can be up to three times the value of the False Claim, plus from $14,308 to $28,619 in fines, per claim (in 2025 which may be amended from time to time). Penalties are increased each year to account for inflation. While state law does not permit private suits like the federal False Claims Act for Medicaid fraud, state law does include either civil or criminal penalties against those who attempt to obtain Medicaid payments to which they are not entitled, or who commit Medicaid fraud.

The False Claims Act protects anyone who files a False Claim lawsuit from being fired, demoted, threatened, or harassed by their employer for filing the suit. If a court finds that the employer retaliated, the court can order the employer to re-hire the employee and to pay the employee twice the amount of back pay that is owed, plus interest and attorney's fees. State law provides equivalent protections from retaliation by an employer for employees who report Medicaid fraud to the authorities.

BSMH Compliance Program supports compliance with the False Claims Act by:

- Monitoring and auditing business activities to prevent or detect errors in coding or billing.
- Educating our associates and vendors that they are responsible to report any concern about a possible False Claim at a BSMH facility via our 3-Step Reporting Process.
- Investigating all reported concerns and correcting any billing errors discovered.
- Protecting our associates and vendors from adverse action when they do the right thing and report any genuine concern via the 3-Step Reporting Process. BSMH will investigate any allegation of retaliation against an associate for speaking up.

ATTACHMENT 2

BON SECOURS MERCY HEALTH

STATEMENTS OF SOCIAL IMPERATIVES

Consistent with its Mission and Values, the Bon Secours Mercy Health Ministry identifies the following key social imperatives as urgent issues for the community of Bon Secours Mercy Health, the communities served by Bon Secours Mercy Health, and its Vendor Partners.

Dignity & Unity

BSMH embraces treating individuals with dignity and respecting each person's unique gifts, talents, and attributes in their contributions to the work force. It is essential that we promote the unity of people coming from a broad range of social, ethnic, and demographic backgrounds, including disabilities, races, national origins, ages, religious preferences, genders, and sexual orientations in our work force and we encourage our vendors to do the same.

Human Trafficking, Forced Labor, & Child Labor

BSMH will not tolerate human trafficking, forced labor, and child labor anywhere in its supply chain. BSMH will aggressively monitor its vendor population and will immediately terminate any vendor relationships where evidence of human trafficking, forced labor, and child labor is discovered. BSMH demands that all our Vendor Partners take an equally definitive position on these reprehensible practices through the adoption of policies and practices.

Protecting Our Earth.

BSMH recognizes that the resources of our earth are finite and that the viability and ultimately survival of mankind requires concerted ongoing environmental stewardship. Toward that end, BSMH takes active measures to use earth resources wisely through recycling, energy conservation, and embracing the application of environmentally friendly resource harvesting, manufacturing, and distribution processes. This commitment must be shared globally, and accordingly, BSMH gives preference to Vendors Partners who have substantive measurable programs for environmental stewardship.

ATTACHMENT 3

INFORMATION SECURITY GUIDELINES

I. Definitions. Except as otherwise modified or defined herein, all capitalized terms in this **Attachment** have the same meanings as set forth in the underlying agreement, and amendments, exhibits, and Attachments thereto, to which this **Attachment** is attached ("**Agreement**").

II. Secure Protection and Handling of Data. Vendor acknowledges and agrees that all Customer's Confidential Information shall be subject to this **Attachment**.

III. Comprehensive Information Security Program. Vendor acknowledges and affirms that: (a) it has and maintains a written comprehensive information security program ("**CISP**") containing appropriate administrative, technical and physical safeguards for the security, confidentiality and integrity of Customer's Confidential Information; and (b) that the CISP is periodically reviewed and appropriate updates are implemented to address any gaps identified in the CISP. Vendor agrees to make the CISP, including all relevant policies and procedures thereunder, available to Customer upon reasonable request.

To the extent that Vendor will have access to Protected Health Information, the CISP shall, at minimum, meet the standards set forth in and comply with:

- Sections 261 through 264 of the federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, 45 CFR Part160 and Subparts A and C of Part164 (the "**HIPAA Security Rule**"), and 45 CFR Part 160 and Subparts A and E of Part 164 ("**HIPAA Privacy Rule**"); and
- the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5), Title XIII of Division A and Title IV of Division B, called the "Health Information Technology for Economic and Clinical Health" ("**HITECH**") Act; and regulations promulgated thereunder by the U.S. Department of Health and Human Services (the "**HIPAA Regulations**") and other applicable laws.

IV. Network Security. Vendor agrees at all times to maintain network security that – at a minimum – includes: network firewall with secure access control list configurations, intrusion detection and prevention. Vendor agrees to implement endpoint security that includes at a minimum (a) antivirus, (b) advanced malware protection, (c) host intrusion prevention, (d) host firewall, (e) sandboxing with dynamic and static code analysis, (f) artificial intelligence, (g) behavior based analytics, (h) file integrity monitoring, (i) data loss prevention and (j) encryption. Vendor internal network security controls shall include network data loss prevention, security information and event management (SIEM). Vendor agrees to complete annual vulnerability assessments, and penetration tests to validate internal security control effectiveness. Likewise, Vendor agrees to maintain network security that conforms to generally recognized "**Industry Standards**" (set forth below) and best practices, and that Vendor, at a minimum, then applies to its own network. Vendor may not place Customer's Confidential Information, or systems containing Customer's Confidential Information, on any public network.

V. Information Security Risk Management Program. Vendor agrees to implement and maintain an information security risk management program in compliance with the HIPAA Security Rule and Health Information Trust Alliance ("**HITRUST**"), NIST SP 800-30, NIST SP 800-115, PCI-DSS. Risk management program shall include internal and external vulnerability assessments, penetration tests, asset categorization, annual risk assessment, risk management dashboard, and risk register with quantitative and quartile impact for mission critical assets. Mission critical assets shall include Electronic Protected Health Information (EPHI), Personal Identifiable Information ("**PII**"), card holder data, intellectual property, and Internet-connected ("**IoT**") bio-medical, and facility (IoT) (i.e., HVAC, electrical) systems.

VI. Application Security. Vendor agrees at all times to provide, maintain and support its software and subsequent updates, upgrades, and bug fixes such that the software is, and remains, secure from those vulnerabilities as described in:

- The Open Web Application Security Project's ("**OWASP**") "Top Ten Project" – see http://www.owasp.org;

- The CWE/SANS Top 25 Programming Errors - see http://cwe.mitre.org/top25/ or http://www.sans.org/top25-programming-errors/;
- Other generally recognized and comparable industry practices or standards;
- Application whitelisting and inspection with layer seven firewall; and
- Network/Application proxy that provides basic and advanced application network services that include but not limited to load balancing, web performance, optimization, application delivery and secure remote access.

VII. Cloud Security. Vendor agrees to implement internal security controls that support identity and access management, privacy high availability, and access control for cloud computing services. Cloud computing internal security controls shall provide customer data segmentation, zone based security isolation, data leakage and deletion protection, backup/ business continuity, and encryption.

VIII. Incident Response. Vendor agrees and shall implement a cyber security incident response program in compliance with NIST SP 800-61, PCI-DSS, HITRUST, and the HIPAA Security Rule.

IX. Data Security. Vendor agrees to preserve the security, integrity and confidentiality of Customer's Confidential Information with administrative, technical and physical measures that conform to generally recognized industry standards (see Industry Standards) and best practices that Vendor then applies to its own processing environment. Maintenance of a secure processing environment includes, but is not limited to, the timely application of patches, fixes and updates to operating systems and applications as provided by Vendor or open source support. Vendor expressly agrees to:

- Limit access to Customer's Confidential Information to those employees who have a legitimate business need to know or access the information;
- Prohibit disclosure of any social security numbers included in Customer's Confidential Information, except as expressly permitted by the Agreement; and
- Restrict remote access to Customer's Confidential Information.

X. Data Storage. Vendor agrees that any and all Customer's Confidential Information will be stored, processed, and maintained solely on designated target servers and that no Customer's Confidential Information at any time will be processed on or transferred to any portable or laptop computing device or any portable storage medium, unless that device or storage medium is in use as part of Vendor's designated backup and recovery processes and encrypted in accordance with Data Encryption, herein. Any transmission, transportation, or storage of Customer's Confidential Information outside the United States is prohibited except on prior written authorization by Customer. Vendor agrees to store data for six years in compliance with the HIPAA Security Rule and HIPAA Privacy Rule, Parts 164.31(b)(1),164.316(b) (2) and PCI-DSS audit log creation/ deletion of system-level objects for one year; ninety (90) days immediately available, if applicable.

XI. Data Transmission. Vendor agrees that any and all electronic transmission or exchange of Customer's Confidential Information with Customer and/or any other parties expressly designated by Customer shall take place via secure means (*e.g.*, SSH, SSL, SFTPS, TLS, IPSec) and solely in accordance with Data Re-Use, as described below.

XII. Data Encryption. Vendor agrees to store all Customer backup data as part of its designated backup and recovery processes in encrypted form, using a commercially supported encryption solution. Vendor further agrees that any and all Customer's Confidential Information stored on any portable or laptop computing device or any portable storage medium be likewise encrypted. Encryption solutions will be deployed with no less than a 128-bit key for symmetric encryption and a 1024 (or larger) bit key length for asymmetric encryption.

XIII. Data Re-Use. Vendor agrees that any and all Customer's Confidential Information shall be used expressly and solely for the purposes enumerated in the Agreement. Customer's Confidential Information shall not be distributed, repurposed or shared across other applications, environments, or business units of Vendor. Vendor further agrees that no Customer's Confidential Information of any kind shall be transmitted, exchanged or otherwise passed to other vendors or interested parties except on a case-by-case basis as specifically agreed to in writing by Customer.

XIV. End of Agreement Data Handling. Vendor agrees that during the term of the Agreement, and following termination or expiration of the Agreement to the extent Vendor retains Customer's Confidential Information, Vendor shall ensure that no Security Breach (defined below) occurs and shall follow Customer instructions as to the preservation, transfer, or destruction of Customer's Confidential Information as further described in the Agreement.

XV. Security Breach Notification Vendor agrees to comply with all applicable laws that require the notification of individuals in the event of a Security Breach or other event requiring notification. If Vendor has knowledge or a reasonable belief that a Breach has occurred or may have occurred, Vendor shall notify the Customer in accordance with the requirements of 45 CFR § 164.410, "**Security Breach**" means any actual or potential loss or unauthorized acquisition, access, or use of Customer's Confidential Information or a Breach (as defined in 45 CFR 164.402). In the event of a Security Breach, Vendor agrees to notify Customer in accordance with applicable law, and in addition, shall notify Customer as follows:

- Notify Customer by calling Customer's Help Desk (in service 24/7) at **1-833-MY1HELP (1-833-691-4357)**;
- Comply with Vendor's obligations under that certain Business Associate Agreement by and between the parties; and
- Indemnify, hold harmless and defend Customer and its Affiliates and their trustees, officers, employees, and agents from and against any claims, damages, or other harm related to such Security Breach and notice requirements.

XVI. Assurance. Vendor will annually provide Customer with an external, independent attestation of their information security controls environment. This attestation of control effectiveness should include a SSAE16 SOC 1 Controls review and SSAE16 SOC2 Type2 Control Reviews focusing on Security, Availability, Confidentiality, Processing Integrity or Privacy. Reviews such as a HITRUST, PCI-DSS, and ISO27001 are acceptable substitutes for the SSAE16 SOC2 Type 2 reporting requirement. Customer has the right to request additional controls to be added to the certified SSAE16 SOC2 Type2 review for testing of controls that impact Customer's Confidential Information, systems, and services.

XVII. Right to Audit. Vendor agrees to permit Customer or appointed/designated Customer auditor firm ("**Auditors**") right to audit and or perform a risk assessment in compliance with the HIPAA Security Rule, HITRUST, NIST SP 800-30, NIST SP 800-115. Risk assessment shall include vulnerability assessments, penetration testing, security/standardized information gathering questionnaire ("**SIG**"). Vendor agrees to provide Customer, upon request and within 10 business days' notice to Vendor, internal/external vulnerability assessment reports, penetration assessment reports, information security policies and standards, audit attestation of compliance and/or certification reports (e.g., SOC 2 Type 2, HITRUST, HIPAA, ISO27001, PCI-DSS).

If the documentation requested cannot be removed from Vendor's premises, Vendor will allow the Auditors access to Vendor's, or its applicable sub-vendor's or affiliate's, site(s). Where necessary, Vendor will provide a personal site guide for the Auditors while on site. Vendor will provide a private accommodation on site for data analysis and meetings; the accommodation will allow for a reasonable workspace, with appropriate lighting, electrical outlets, a printer and Internet connectivity. Vendor, or its applicable sub-vendor or affiliate, will make necessary employees or contractors available for interviews in person or on the phone during the time frame of the audit. Audits will be at Customer sole expense, except where the audit reveals material noncompliance with contract specifications, in which case the cost will be borne by Vendor.

XVIII. Industry Standards. Generally recognized industry standards include but are not limited to the current standards and benchmarks set forth and maintained by:

- Center for Internet Security - see http://www.cisecurity.org
- Payment Card Industry/Data Security Standards (PCI/DSS) – see https://www.pcisecuritystandards.org/pci_security/
- National Institute for Standards and Technology - see http://csrc.nist.gov
- Federal Information Security Management Act (FISMA) - see http://csrc.nist.gov
- Federal Trade Commission (FTC) – see http://business.ftc.gov/privacy-and-security/data-security
- Organization for the Advancement of Structured Information Standards (OASIS) – see http://www.oasis-open.org
- Health and Human Services (HHS) – see http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html

XIX. Remote Access Standards. To the extent Vendor accesses Customer's network, Vendor must comply with Customer's remote access standards. Customer monitors all remote access connections to/from Customer's network and reserves the right to deny and/or revoke remote access to any Customer to maintain the security and integrity of Customer's systems.

XX. Medical Device Security. If Vendor is supplying a medical device pursuant to the Agreement, then Vendor agrees to submit a Manufacturer Disclosure Statement for Medical Device Security ("**MDS2**") to Customer, and Vendor shall comply with the terms and conditions set forth in this Section:

- Vendor acknowledges and affirms that the information disclosed by Vendor and submitted to Customer in the MDS2 relating to this Agreement is complete and accurate.
- If at any time Vendor discovers or has reason to believe that the information contained in the MDS2 is no longer accurate and/or complete, Vendor shall immediately notify Customer and provide a description of the inaccurate and/or incomplete information.
- Vendor agrees to comply with current guidance documents issued by the FDA relating to the security of medical devices that store, transmit or otherwise process data (*e.g.*, "*Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software*" (2005)) in the development, implementation and maintenance (as applicable) of such medical device(s) subject to this Agreement.
- Vendor agrees to permit Customer to implement Sential Biomedical Awareness and Alert ("**SBAAP**") enhanced security architecture for internet connected (IoT) bio-medical hardware. Vendor agrees to follow Customer bio-medical (IoT) connected hardware security policy, incident response policy and onboarding procedure.

ATTACHMENT 4

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (the "**BAA**") is by and between Bon Secours Mercy Health, Inc. ("**BSMH**") (on behalf of itself and its covered entity affiliates, collectively, "**Covered Entity**") and Vendor identified in the Purchase Order ("**Business Associate**").

BACKGROUND

A. Business Associate and Covered Entity are parties to an agreement (the "**Underlying Agreement**") pursuant to which Business Associate provides certain services (the "**Services**") to Covered Entity. In connection with Business Associate providing the Services to Covered Entity, Covered Entity discloses to Business Associate certain Protected Health Information (as defined below) of patients, residents or other BSMHs of Covered Entity.

B. By providing the Services to Covered Entity pursuant to the Underlying Agreement, Business Associate acknowledges that it is acting as a Business Associate of Covered Entity, as defined by the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**") and its implementing regulations as amended and in effect.

C. In order to ensure that Covered Entity is in compliance with HIPAA and other applicable federal and State laws and regulations regarding the disclosure of PHI to Business Associate, the parties have agreed to enter into the BAA.

1. Definitions. Capitalized terms not otherwise defined in the BAA shall have the same meaning as those terms in the HIPAA Privacy Rule and Security Rule.

A. "**Breach**" when capitalized, "Breach" shall have the meaning set forth in 45 CFR § 164.402 (including all of its subsections); with respect to all other uses of the word "breach" in the BAA, the word shall have its ordinary contract meaning.

B. "**Electronic Protected Health Information**" or "**EPHI**" shall have the same meaning as the term "electronic protected health information" in 45 CFR § 160.103, limited to information that Business Associate creates, accesses or receives on behalf of Covered Entity.

C. "**Protected Health Information**" or "**PHI**" shall have the meaning set forth in the Privacy Rule, limited to information that Business Associate creates, accesses or receives on behalf of Covered Entity. PHI includes EPHI.

D. "**Privacy Rule**" means the Standards for Privacy of Individually Identifiable Health Information, codified at 45 CFR parts 160 and 164, Subparts A, D and E, as currently in effect.

E. "**Security Rule**" means the Standards for Security for the Protection of Electronic Protected Health Information, codified at 45 CFR parts 160 and 164, Subpart C, as currently in effect.

F. "**Unsecured Protected Health Information**" shall have the same meaning as the term "unsecured protected health information" in 45 CFR § 164.402, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

2. Scope of Use and Disclosure of PHI**.**

2.1 Business Associate Status. Business Associate acknowledges and agrees that it is a "Business Associate" as defined by HIPAA. As a Business Associate of Covered Entity, Business Associate shall, in addition to complying with the other terms and conditions of the Underlying Agreement, comply with the HIPAA-required provisions set forth in the BAA and more stringent applicable State law. In the event of a conflict between the terms of the BAA and the Underlying Agreement with respect to the use or disclosure of PHI, the terms of the BAA will govern. In all other circumstances, the terms of the Underlying Agreement will govern.

2.2 Performance of Services. Business Associate may use PHI only to perform the Services and its other obligations pursuant to the Underlying Agreement or as Required by Law. Business Associate may disclose such PHI only within its organization and

only to those of its employees who need to know such information in order to perform its obligations under the Underlying Agreement and, in such case, only the minimum amount of such PHI as is necessary for such performance. Business Associate shall not access, use or disclose PHI in any manner that would violate HIPAA if such access, use or disclosure was done by Covered Entity.

2.3 Privacy Rule Obligations. Business Associate shall comply with the Privacy Rule as it directly applies to business associates. To the extent Business Associate carries out one or more of Covered Entity's obligations under the HIPAA Privacy Rule, Business Associate shall comply with the requirements of HIPAA that apply to Covered Entity in the performance of such obligation(s).

2.4 Safeguards for Protection of PHI. Business Associate agrees that it will (a) protect and safeguard from any disclosure (whether oral, written or otherwise) all PHI with which it may come into contact with in accordance with HIPAA and more stringent state laws and regulations governing the handling of such information; and (b) use appropriate safeguards to prevent use or disclosure of PHI other than as permitted by the Underlying Agreement or the BAA or as Required by Law.

2.5 Statistical Aggregation. Business Associate agrees that its obligations under the BAA include, without limitation, its agreement that it shall not use any PHI obtained from Covered Entity to compile or distribute any statistical analyses or reports utilizing aggregate data or for any commercial purpose whatsoever (e.g., sell or transfer for value to a third party such aggregated or de-identified data), unless permitted pursuant to the purposes of the Underlying Agreement or otherwise permitted by Covered Entity in a written document.

2.6 Disclosure to Subcontractors. Business Associate shall ensure that any and all subcontractors that create, receive, maintain or transmit PHI on behalf of Business Associate agree, in writing, to the same terms and conditions of the BAA with respect to PHI. Business Associate shall make such agreements with its subcontractors available upon request of Covered Entity.

2.7 Required Disclosure. If Business Associate is confronted with legal action to disclose any PHI, Business Associate shall notify Covered Entity within two (2) business days of such obligation and assist Covered Entity (at Covered Entity's expense) in obtaining a protective order or other similar order and shall thereafter disclose only the minimum amount of PHI that is required to be disclosed in order to comply with the legal action, whether or not a protective order or other order has been obtained.

2.8 Notification. Without unreasonable delay, Business Associate shall notify Covered Entity, in writing, of any use or disclosure of PHI outside the purpose of the BAA or the Underlying Agreement of which Business Associate becomes aware. Without unreasonable delay, Business Associate shall report to Covered Entity in writing of any Security Incident of which it becomes aware. In addition, upon Covered Entity's request, Business Associate shall provide a report of any and all impermissible uses, disclosures, and/or Security Incidents.

2.9 Mitigation. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate or a subcontractor or agent of Business Associate in violation of the requirements of the BAA, the Underlying Agreement, the Privacy Rule, the Security Rule or other applicable federal or state law.

2.10 Injunctive Relief. Business Associate acknowledges that disclosure of any PHI without Covered Entity's prior written consent would cause continuing, substantial and irreparable injury to Covered Entity and that Covered Entity's remedies at law for such disclosure will not be adequate. Accordingly, Business Associate agrees that Covered Entity shall be entitled to immediate injunctive relief against the breach or threatened breach of the foregoing undertakings by Business Associate, and that such rights shall be in addition to, and not in limitation of, any other rights or remedies to which Covered Entity may be entitled at law or equity.

2.11 Security. Business Associate shall comply with the Security Rule as amended and in effect, as it directly applies to business associates. Business Associate shall implement and maintain Administrative Safeguards, Physical Safeguards and Technical Safeguards that reasonably and appropriately protect the Confidentiality, Integrity and Availability of EPHI; provided that, at a minimum, Business Associate's safeguards will include all "Required" Implementation Specifications contained in the Security Rule, including any subsequent amendments and regulations promulgated thereunder. If in performing it obligations under the BAA or the Underlying Agreement, Business Associate, its employees, agents, subcontractors and any other individual permitted by Business Associate will have access to any computer system, network, file, data or software owned by or licensed to Covered Entity that contains PHI, Business Associate shall use industry best security practices and shall take all reasonable security measures necessary to protect the security of all such computer systems, networks, files, data and software.

2.12 Patients' Rights.

A. Patients' Right to Review. Business Associate shall make PHI maintained in a Designated Record Set available to Covered Entity or, at the direction of Covered Entity, to an Individual, in accordance with §164.524 of the Privacy Rule.

B. Patient Right to Amend. Business Associate shall make PHI available for amendment and incorporate any amendments to PHI maintained in a Designated Record Set at the direction of Covered Entity and in accordance with §164.526 of the Privacy Rule. Covered Entity shall be involved in any decision of Business Associate to amend the PHI of an Individual.

C. Patient Right to Request Accounting. Business Associate shall document and make available to Covered Entity or, at the direction of Covered Entity, to an Individual, information relating to such Individual as is necessary for Covered Entity to respond to a request for an accounting of disclosures in accordance with §164.528 of the Privacy Rule.

i. Business Associate agrees to implement an appropriate record keeping process to enable it to comply with the requirements of this Section.

ii. Business Associate agrees to provide PHI it maintains electronically in a Designated Record Set in an electronic form at the request of Covered Entity or an Individual.

2.13 Notice to Covered Entity. Business Associate shall notify Covered Entity immediately in writing upon receiving a request from an Individual to review, copy or amend his or her medical record information or to receive an accounting of uses and disclosures. Business Associate shall also provide Covered Entity with a prompt written report of the details of its handling of such requests.

2.14 Access. Until the expiration of four (4) years after the furnishing of Services pursuant to the Underlying Agreement, Business Associate will make available to the Secretary, U.S. Department of Health and Human Services and the U.S. Comptroller General, and their representatives, the BAA, the Underlying Agreement and all books, documents and records necessary to certify the nature and extent of the costs of those services. If Business Associate carries out any of its duties pursuant to the BAA or the Underlying Agreement through a subcontract worth $10,000 or more over a 12-month period with a related organization, the subcontract will also contain an access clause to permit access by the Secretary, Comptroller General and their representatives to the related organization's books and records.

2.15 Breach. If Business Associate has knowledge or a reasonable belief that a Breach of Unsecured Protected Health Information has occurred or may have occurred, Business Associate shall notify the Covered Entity in accordance with the requirements of 45 CFR § 164.410. For avoidance of doubt, Business Associate shall notify Covered Entity if it has knowledge of a potential Breach so that Covered Entity may determine and confirm whether a Breach has occurred. Such notification shall include, to the extent possible, the identification of each Individual whose PHI has been or is reasonably believed to have been accessed, acquired, used or disclosed during the Breach, along with any other information that the Covered Entity will be required to include in its notification to the Individual, the media and/or the Secretary, as applicable, including, without limitation, a description of the Breach, the date of the Breach and its discovery, the types of Unsecured Protected Health Information involved and a description of Business Associate's investigation, mitigation and prevention efforts. Business Associate agrees to coordinate immediately with Covered Entity in the event that Breach notifications to individuals, government agencies and/or media outlets are required; provided however, that, at the option of Covered Entity and with Covered Entity's approval of all written notices, Business Associate shall make such notifications to individuals, government agencies and/or media outlets.

2.16 Minimum Necessary. Business Associate agrees to follow any guidance issued by HHS regarding what constitutes "minimum necessary" with respect to the use or disclosure of PHI as well as the policies and procedures of Covered Entity. Until the time that any such guidance is issued, Business Associate shall limit its use or disclosure of PHI, to the extent practicable, to the limited data set (as defined in Section 45 CFR § 164.514(e)(2)) or, to the minimum necessary to accomplish the intended purpose of such use, disclosure or request, respectively. Business Associate warrants and represents that each of the data

elements of any PHI that it may access on behalf of Covered Entity is minimally necessary to permit Business Associate to provide the services under the BAA.

2.17 No Sale of PHI. As Covered Entity has not secured individual authorization from the patients whose PHI is contemplated for use under the BAA, Business Associate is prohibited from directly or indirectly exchanging the Covered Entity's PHI for remuneration with any other person or entity.

3. Term and Termination.

3.1 Term. The BAA shall become effective as of the effective date of the Underlying Agreement ("**Effective Date**") and remain in effect until all PHI is returned or destroyed in accordance with Section 3.3 of the BAA.

3.2 Termination for Failure to Comply. Covered Entity may terminate the BAA and the Underlying Agreement immediately if Covered Entity in its sole discretion determines that Business Associate has violated a material term of the BAA. Covered Entity, at its option and within its sole discretion, may (a) take steps to cure the breach; and (b) in the event of such a cure, elect to keep the BAA in force.

3.3 Effect of Termination; Return or Destruction of Covered Entity's PHI. Upon termination of the Underlying Agreement for any reason and except as required by law, Business Associate will return or destroy (as agreed to with Covered Entity) all PHI within thirty (30) days of the date of termination. Business Associate shall certify in writing that such PHI has been destroyed in accordance with its obligations under this Section. Business Associate shall accomplish the destruction of BSMH's Confidential Information by "purging" or "physical destruction", in accordance with the National Institute of Standards, Guidelines for Media Sanitization, SP800-88, Appendix A - see http://csrc.nist.gov/.

4. Limitation of Liability, Indemnification and Insurance.

4.1 Limitation of Liability. To the extent that Business Associate has limited its liability under the terms of the Underlying Agreement, whether with a maximum recovery for direct damages or a disclaimer against any consequential, indirect or punitive damages, or other such limitations, all limitations shall exclude all damages to Covered Entity arising out of the acts or omissions of Business Associate arising under or relating to: (i) any inappropriate release or misuse of PHI by Business Associate, its employees, agents or subcontractors; (ii) any breach of the confidentiality provisions contained in the BAA or the Underlying Agreement by Business Associate, its employees, agents or subcontractors; or (iii) any violation by Business Associate, its employees, agents or subcontractors of any state or federal law or regulation governing the protection of protected health information.

4.2 Indemnification. Notwithstanding any limitation of liability provisions contained in the Underlying Agreement and, in addition to any other indemnification provisions contained in the Underlying Agreement, Business Associate agrees to indemnify, defend and hold harmless Covered Entity (and its parents, officers, directors, members, stockholders, subsidiaries, affiliates and agents) from and against any liability, claim, action, loss, cost, damage or expense incurred or suffered by Covered Entity, directly or indirectly, arising out of the acts and omissions of Business Associate arising under or relating to: (i) any inappropriate release or misuse of PHI by Business Associate, its employees, agents or subcontractors, including any Breach of PHI; (ii) any breach of the confidentiality provisions contained in the BAA or the Underlying Agreement by Business Associate, its employees, agents or subcontractors; or (iii) any violation by Business Associate, its employees, agents or subcontractors of any state or federal law or regulation governing the protection of protected health information.

5. Miscellaneous.

5.1 Notices. Any notice required or permitted under the BAA will be given in writing in accordance with, and to the notice address contained in, the Underlying Agreement.

5.2 Governing Law. The BAA will be governed by, and construed in accordance with the laws of the state of Ohio. Venue is Hamilton County.

5.3 Waiver. No delay or omission by either party to exercise any right or remedy under the BAA will be construed to be either acquiescence or the waiver of the ability to exercise any right or remedy in the future.

5.4 Severability. In the event any part or parts of the BAA are held to be unenforceable, the remainder of the BAA will continue in effect.

5.5 Modification or Termination Upon Advice of Counsel. If at any time either party reasonably believes in good faith based upon the advice of reputable health care counsel that the BAA or the performance by that party of any of its obligations under the BAA violates any material law or regulation, state or federal, presents a substantial risk of the loss or restriction of that party's license, tax exemption, or right to participate in Medicare, Medicaid, or any other governmental program or presents a substantial risk of causing debt issued by that party that was tax-exempt when originally issued to become subject to federal or state income tax, then that party may, upon written notice, require the other party to enter into good faith negotiations to renegotiate the terms of the BAA, in a manner that attempts to retain as much as possible of the economic arrangements originally contemplated by the parties without violating any applicable legal, tax or reimbursement requirements. If the parties are unable to reach an agreement concerning the modification of the BAA within 60 days after the date of the notice seeking renegotiation (or sooner if required by law), then either party may immediately terminate the BAA by written notice to the other party. The rights of the parties under this Section are in addition to any other termination rights the parties may have under the BAA.

5.6 Amendments. The BAA may not be modified in any respect other than by a written instrument signed by both parties.