BANNER SECURITY ADDENDUM

The terms and conditions of this Security Addendum ("Addendum") apply to vendors and business partners ("Contractor") providing services that include Processing Banner Content under an underlying agreement ("Agreement"). By signing the Agreement, Contractor agrees to the terms and conditions of this Addendum as may be amended as described below. This Addendum establishes the minimum standards to protect the Banner Systems and Banner Content and to minimize security risks and costly data breaches.

1. PROTECTION OF BANNER CONTENT. Contractor will establish and maintain practices, procedures and other safeguards to prevent the unauthorized access, destruction, loss, alteration or disclosure of Banner Content in the possession of the Contractor or Contractor Personnel. These practices will conform to the terms of this Addendum, the Agreement and Applicable Laws.

1.1 Contractor's Obligations. Contractor will hold, maintain, and manage Banner Content in strictest confidence and use reasonable care to prevent any unauthorized use or disclosure. Contractor will not use, assign, sell, rent, lease, license, transfer, convey, distribute, or otherwise disclose or make available Banner Content for Contractor's own purposes or for the benefit of any party other than Banner without Banner's prior express written consent. Contractor represents that during the term of the Agreement it will maintain and implement a comprehensive written information security program that complies with Applicable Laws and relevant Standards. Contractor's information security program will include appropriate administrative, technical, physical, organizational, and operational safeguards and other security measures that will: (a) establish minimum controls and requirements consistent with Standards to be met in connection with the safeguarding of Banner Content in any form; (b) ensure the security, integrity, confidentiality, and availability of Banner Content, the Banner Systems managed by Contractor, and the Contractor Systems Accessing or Processing Banner Content in a manner consistent with Standards; (c) protect against anticipated threats or hazards to the security and integrity of Banner Content and the Contractor Systems; (d) identify, report, and notify Banner of an Incident; (e) investigate and remediate an Incident; and (f) provide Banner with satisfactory assurance that such Incident will not recur.

1.2 Data Management Obligations. Unless otherwise provided in a Business Associate Agreement between the parties, ***if*** Contractor stores Banner Content, (a) Contractor will implement and maintain information management requirements and policies and establish procedures to ensure compliance with the terms of this Addendum; and (b) promptly upon the expiration or termination of the Agreement or upon reasonable written request, and at no additional cost to Banner, Contractor will, at Banner's election, either (i) securely destroy or render unreadable, or (ii) return to Banner all Banner Content received by the Contractor. If Banner Content is returned to Banner, Contractor will deliver a complete and secure file of Banner Content in a file format agreed upon by the parties. If complete data destruction or return is not technically feasible or retention is required by Applicable Laws or Standards (excluding instances when Banner Content is retained as part of Contractor's automatic, secured back-up or similar archival system), Contractor will notify Banner in writing of Contractor's inability to destroy or return Banner Content, and will continue to protect Banner Content according to the requirements set forth in this Addendum.

1.3 Contractor Personnel Requirements. Contractor will limit Access to Banner Content to those who have a need to know and ensure that Contractor Personnel receive appropriate training regarding the security requirements set forth in this Addendum and comply with provisions that are no less restrictive than those required by this Addendum.

1.4 Third Party Requirements. Contractor will not assign **all** its rights or obligations under this Addendum to a third party(ies) without the prior written consent of Banner. If Contractor subcontracts **any** rights or obligations, Contractor will enter into a written agreement with each third party that imposes obligations that are no less restrictive than those imposed on Contractor under this Addendum. Contractor will only retain third

parties that Contractor reasonably expects are suitable and capable of securing Banner Content in accordance with this Addendum, the Agreement, and Banner's written instructions.

1.5 Subpoena, Judicial, and Administrative Disclosure Orders. To the extent not prohibited by law, rule or order, Contractor will notify Banner promptly in writing of any subpoena or other judicial or administrative order by a government authority or proceeding seeking access to or disclosure of Banner Content prior to responding to such request. Banner will have the right to defend such action in lieu of and on behalf of Contractor at Banner's expense. Banner may seek a protective order and Contractor will reasonably cooperate with Banner in such efforts.

1.6 Incident Notification. Contractor shall notify Banner within three business days of discovery of any Incident. In addition to providing notice, Contractor will: (a) inform Banner in writing of any Incident; (b) summarize in reasonable detail the impact on Banner; (c) identify and take reasonable and necessary corrective action(s); and (d) cooperate fully with Banner in all reasonable and lawful efforts to prevent, investigate, mitigate, report, or rectify such Incident. Contractor will not distribute any filings, communications, notices, press releases, or reports related to any Incident that materially impacts Banner, Banner Content, or the Banner Systems without prior written approval from Banner, which will not be unreasonably withheld or delayed.

1.7 Notification Costs. Upon the occurrence of an Incident for which Contractor is responsible, Contractor will reimburse Banner for reasonable expenses incurred by Banner, including, without limitation, expenses in notifying individuals affected by the breach, providing protective services, and undertaking other actions that may be required under Applicable Law. Notification costs will be at Banner's discretion and are subject to any limitation of liability provisions agreed to by the parties to the Agreement.

1.8 Compliance. Contractor agrees to comply with Applicable Laws and Standards. Contractor covenants and agrees that no Applicable Law, legal requirement, or privacy or information security enforcement action, investigation, litigation, claim, or any other circumstance (collectively, "Action") prohibits Contractor from: (a) fulfilling its obligations under this Addendum or (b) complying with written instructions it receives from Banner concerning the Processing of Banner Content. If any Action is reasonably likely to adversely affect Contractor's ability to fulfill or comply with its obligations under this Addendum, Contractor will, within five business days, notify Banner in writing. If Contractor fails to remedy any curable Action pursuant to any cure provision provided in the Agreement or as reasonably directed by Banner, Banner may, without penalty: (i) suspend Access or Processing, (ii) terminate Access or Processing, and/or (iii) terminate the Agreement.

2. ACCESS TO THE BANNER SYSTEM AND BANNER CONTENT.

2.1 Restrictions. Except as specifically contemplated in the Agreement, Contractor will not, and will not allow any Contractor Personnel to: (a) Process Banner Content or Personal Information from outside the United States; (b) attempt unauthorized Access to Banner Content; (c) input, delete, or otherwise modify Banner Content or make any changes to the Banner Systems; or (d) Access, or attempt to Access, any third party networks or systems from the Banner Systems except as necessary to perform the Services and agreed to in writing by the parties.

2.2 Portable Storage Media. Unless expressly authorized in writing by Banner, Contractor will not allow any Personal Information to be Processed using laptops, USB drives, external hard drives, mobile devices, or any other portable storage media (collectively, "**Portable Storage Media**"), except as required to perform the Services and only for the duration necessary. Where Portable Storage Media is used, Contractor will use industry-standard encryption.

2.3 Credentials. Banner may issue Contractor Personnel: (a) a login ID, password, or other authentication credentials; or (b) a Banner facility identification card or other physical security access or

permission (collectively, "**Credentials**"), as necessary to perform the Services. Contractor Personnel will treat Credentials with due care and confidentiality to prevent unauthorized disclosure or misuse. Contractor acknowledges that any Credentials issued to Contractor Personnel are Banner's confidential information subject to the protections set forth in this Addendum, and will not be shared, disclosed, or used in any unauthorized manner. Contractor will be responsible for the actions of any individuals using Credentials issued to Contractor Personnel. Upon termination of the Services or the underlying Agreement, Contractor will promptly return physical Credentials. Contractor will notify Banner, where possible, in advance or as soon as reasonably possible if any Contractor Personnel no longer require their Credentials.

2.4 Security Design Information. Any information related to the design or security topology of the Banner Systems acquired by Contractor or that may be gained through Contractor's Access will constitute Banner Content. Contractor will not share, disclose, or use such information in any manner, unless expressly authorized by Banner in writing.

2.5 Remote Access. If the Services require or provide remote Access to the Banner Systems or the Contractor Systems Processing Banner Content, Contractor will secure transmissions of Banner Content using industry-standard encryption technology. Contractor will implement and enable two-factor authentication to remotely access the Contractor Systems that Process Banner Content. If the Contractor Systems provide Banner Consumers with remote Access to the Contractor Systems Processing Banner Content, Contractor will implement two-factor authentication and provide Banner Consumers the option to opt-in to two-factor authentication.

2.6 Malware. Contractor will take reasonable precautions to prevent transmission of a computer virus, malware, trojan, worm, ransomware, or other malicious code (collectively, "**Malware**") to the Banner Systems, Banner personnel, or Banner Consumers. Contractor will maintain current industry standard endpoint protection and detection tools on the Contractor Systems and will ensure Contractor Systems are maintained with up-to-date security patches, hotfixes, and other similar software or firmware changes. Contractor Personnel using the Contractor Systems to deliver the Services will comply with this Addendum. Contractor will notify Banner promptly if Malware is detected in a file or transmission sent to or received from Banner. If Malware is transmitted by Contractor in the delivery of the Services to Banner, Contractor will make reasonable efforts to restore and/or reconstruct Banner Content in Contractor's possession lost due to such Malware at no additional cost to Banner.

2.7 Background Investigations. Contractor will conduct adequate screening of Contractor Personnel, as may be agreed to in the Agreement. Banner reserves the right to restrict or deny Access to Banner facilities, Banner Content and the Banner Systems by any individual for any reason.

3. AUDIT RIGHTS.

3.1. Banner Systems. Contractor and Contractor Personnel may be subject to monitoring and their activity recorded with no advance warning while using the Banner Systems. Contractor consents to such monitoring and recording for itself and Contractor Personnel.

3.2. Audit Rights / Reports. If Contractor Processes Banner Content using Contractor Systems, Banner will have the right to perform an assessment, audit, examination, or review of Contractor's physical and/or technical environment, and/or request Reports to confirm compliance with this Addendum no more than once per calendar year, unless Banner becomes aware of an Incident or raises a reasonable concern regarding Contractor's privacy and/or security practices. Any audit will be: (a) conducted upon reasonable notice; (b) performed during Contractor's normal business hours; and (c) conducted in a manner that minimizes disruption to Contractor's operations. Such audit may be conducted by Banner or its designated representatives who have entered into appropriate confidentiality agreements with Contractor. Contractor will provide reasonable cooperation and reasonable access to Contractor facilities, Contractor Systems and Contractor Personnel. Contractor will respond

promptly to reasonable inquiries from Banner or its designated representatives. If Banner requests Reports, such Reports will be treated as Contractor's confidential information and will be provided at no cost to Banner.

3.3. Third-Party Data Center. If Contractor uses a third-party hosted data center (e.g., Amazon Web Services, Microsoft Azure, Rackspace) to deliver the Services, Contractor will provide Banner with or access to an independent security certification (e.g., SOC 2 or SOC 3) confirming the third-party hosted data center meets or exceeds industry-recognized data center security and availability standards.

3.4. Security Questionnaire. Upon Banner's request to confirm compliance with this Addendum, Applicable Laws, and Standards, Contractor will promptly cooperate and accurately complete a written information security questionnaire provided by Banner or its designated representative regarding Contractor's business practices and information technology environment relating to the Services provided hereunder.

4. AMENDMENT. Banner may modify the terms and conditions of this Addendum at any time and will use reasonable efforts to provide notice if Contractor has provided a current contact and email address. The latest version of the Addendum will be posted on Banner's website.

5. TERMINATION. The following will be considered a material breach giving rise to Banner's right to terminate the Agreement for cause, without penalty: (a) a successful Incident, or (b) Contractor's failure to comply with the material obligations set forth in this Addendum.

6. CONFLICT. In the event of a conflict between the terms of this Addendum and the terms of the Agreement, the order of precedence will be: this Addendum and then the Agreement. If the conflict relates to Personal Information subject to HIPAA and the parties have entered into a Business Associate Agreement ("BAA"), the order of precedence will be: (1) the BAA, (2) this Addendum, and (3) the Agreement.

7. NOTICE. Notification of an Incident will be made promptly (and no later than three business days after discovery) by email to privacy@bannerhealth.com and by courier service with one copy each to Banner's Chief Privacy Officer, Chief Information Security Officer, and General Counsel at 2901 N. Central Avenue, Suite 160, Phoenix, AZ 85012.

8. DEFINITIONS. All capitalized terms used in this Addendum but not defined herein will have the same meaning ascribed to such terms in the Agreement as supplemented by this Addendum.

8.1. "**Access**" or "**Accessing**" means any access to the: (a) Banner Content, (b) the Banner Systems that Process Banner Content, or (c) Banner facilities where Banner Content is Processed.

8.2. "**Applicable Law**" means all federal and state security, confidentiality, and/or privacy and data protection laws, including the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act, and regulations promulgated thereunder ("HIPAA"), and other applicable standards, guidelines, policies, regulations and procedures, as the same may be amended or supplemented from time to time, that are applicable to Contractor, the Services, and/or any other programs or products provided pursuant to the Agreement.

8.3. "**Banner Consumer**" means Banner patients and/or customers.

8.4. "**Banner Content**" means any Personal Information and other Banner confidential information (whether in electronic or non-electronic form) in the care, custody, or control of Contractor or a third party on Contractor's behalf that was (a) provided to Contractor in connection with the Services, or (b) Processed in the course of Contractor's performance of the Services.

8.5. "**Banner Systems**" means any computer, computer network, computer application, storage device, mobile computing device, or software owned or leased by Banner or operated by a third party (excluding Contractor) on Banner's behalf.

8.6. "**Contractor Systems**" means any computer, computer network, computer application, storage device, mobile computing device, or software owned, leased, or controlled by Contractor or operated by a third party on behalf of Contractor.

8.7. "**Incident**" means any actual or reasonably suspected unauthorized Access to or acquisition, alteration, destruction, disclosure, interception, loss, transmission, or use of Banner Content, the Banner Systems, or Banner's confidential information, or delivery of Malware from Contractor to Banner. An Incident does not include minor incidents that regularly occur, such as third-party scans, pings, or unsuccessful attempts to penetrate computer networks or servers maintained by Contractor.

8.8. "**Personal Information**" means any information relating to an identified or identifiable individual (including, but not limited to, name, postal or email address, telephone number, Social Security number, driver's license number, date of birth, demographic information, health or medical information (including Protected Health Information as defined under HIPAA), and financial account information), in whatever format, including that contained in communications, documents, databases, records or materials of any kind whether in individual or aggregate form, and regardless of the media in which it is contained, that may be: (a) disclosed at any time to Contractor or Contractor Personnel by Banner or Banner Personnel in anticipation of, in connection with or incidental to the performance of the Services for or on behalf of Banner; (b) Processed at any time by Contractor or Contractor Personnel in connection with or incidental to the performance of this Addendum or the Agreement; or (c) derived by Contractor or Contractor Personnel from the information described in (a) or (b) above.

8.9. "**Process,**" "**Processed,**" or "**Processing**" means any operation or set of operations performed upon Banner Content, whether or not by automatic means, such as Accessing, adapting, altering, collecting, consulting, creating, disclosing, destroying, maintaining, obtaining, organizing, procuring, receiving, recording, retrieving, storing, transmitting, transferring, or using the data.

8.10. "**Reports**" means a description of the Contractor Systems used to deliver the Services, including the control objectives and related controls applicable to such systems, and an executed copy of one or more opinions or attestations from independent auditors compensated by Contractor that opines on the design and operating effectiveness of information security controls and Contractor's information security program (i.e., SOC 2 Type II, PCI DSS AOC reports (if applicable), etc.).

8.11. **"Standard(s)"** means generally-accepted, industry good practice information security requirements relevant to Contractor's industry and Services.