RIDER 118
INFORMATION SECURITY AND DATA HOSTING AGREEMENT

By accepting the agreement or purchase order to which this Rider 118 (this "Rider") is attached (whether an agreement or purchase order, "Agreement"), Contractor affirms, certifies, and warrants that at all times during the term of the Agreement Contractor will comply with the terms of this Rider and that the representations, statements, and information set forth in this Rider will be current, complete, and accurate. Contractor agrees to provide a certificate of assurance to MD Anderson, on or before each anniversary of the effective date of the Agreement, certifying that the representations, statements, and information set forth in this Rider continues to be current, complete, and accurate and that any updating, testing, or other activities required to be performed on an ongoing or periodic basis have been and are being performed by Contractor in accordance with this Rider.

Contractor agrees that in the event Contractor makes a false statement by affirming, certifying, or warranting that the representations, statements, and information set forth in this Rider or in any annual certificate of assurance are current, complete, and accurate, MD Anderson may, at its option, terminate the Agreement for Contractor's default without further liability, duty or obligation to MD Anderson, and Contractor may be deemed ineligible from participating in future MD Anderson contracts and purchases.

Contractor agrees to notify MD Anderson in writing within thirty (30) days of any changes in the affirmations, certifications, and warranties made by Contractor under this Rider. If MD Anderson, in its reasonable discretion, believes that any changes made by Contractor create an unacceptable level of risk to MD Anderson information assets, MD Anderson may, at its option, terminate the Agreement for Contractor's default without further liability, duty or obligation to MD Anderson, provided that Contractor will first be given notice of MD Anderson's objections to any such change and thirty (30) days to address MD Anderson's concerns to MD Anderson's reasonable satisfaction.

1. **DEFINITIONS:**

1.1 For purposes of this Rider, the terms "Confidential Information" and "Restricted Confidential Information" are defined as follows:

1.1.A Confidential Information is information that, if compromised, would have a significant financial impact to MD Anderson, and violate federal or state law or the terms of confidentiality provisions in MD Anderson contracts. Such information should be accessed only by a limited, authorized group of people as identified by MD Anderson. All data sets that contain "protected health information" as such term is defined in 45 C.F.R. § 160.103 (as such provision is currently drafted and as it is subsequently updated, amended, or revised) ("PHI") receive this classification level, at a minimum.

1.1.B Restricted Confidential Information builds upon the Confidential Information classification by addressing special access needs of a subset of PHI, such as mental health data. Restricted Confidential Information should be accessed only by specific, authorized people as identified by MD Anderson. Only the MD Anderson owner of the data may designate information sets as Restricted Confidential Information or grant access to this data.

2. **COMPLIANCE REQUIREMENTS:**

2.1 If Contractor is providing through or in furtherance of the Agreement cloud computing services or third-party hosted services that store, process, or transmit the data of MD Anderson or another Texas state agency, then Contractor will achieve and maintain compliance and certification of those services with the Texas Risk and Authorization Management Program ("TX-RAMP") throughout the term of the Agreement, unless MD Anderson states in writing that the Agreement is exempt from TX-RAMP or that TX-RAMP is not applicable to the Agreement.

2.2 If Contractor will capture payment card information in its performance of the Agreement, then Contractor will achieve and maintain compliance under the current version of the Payment Card Industry Data Security Standard (PCI DSS) throughout the term of the Agreement.

If Contractor will manage PHI under the Agreement, then Contractor will be compliant with the Health Insurance Portability and Accountability Act (HIPAA) throughout the term of the Agreement.

3. **EVENT NOTIFICATION:**

3.1 Contractor will notify MD Anderson within twenty-four (24) hours of a security event, operational event, or interruption, as defined by MD Anderson's Cybersecurity Operations Manual, and accommodate a site visit or virtual meeting with MD Anderson Cybersecurity or IT personnel for a security audit to resolve corrective and preventative actions.

4. **POLICIES, STANDARDS, AND PROCEDURES:**

4.1 Contractor has and will implement formal, written information security policies ("Information Security Policies") that will protect information assets of MD Anderson, with such Information Security Policies at a minimum covering at least all of the following:

4.1.A Acceptable use;

4.1.B Administrative access;

4.1.C Backup of data and applications;

4.1.D Change management;

4.1.E Computer virus prevention;

4.1.F Email;

4.1.G Encryption requirements;

4.1.H General account management;

4.1.I Identification and authorizations;

4.1.J Internet use;

4.1.K Information owners responsibilities;

4.1.L Information security and information oversight responsibilities;

4.1.M Information system administrator responsibilities;

4.1.N Management of contracted resources;

4.1.O Media control and handling;

4.1.P Network access;

4.1.Q Network scanning;

4.1.R Passwords;

4.1.S Patch management;

4.1.T Physical access;

4.1.U Portable computing and remote access;

4.1.V Risk management program;

4.1.W Security awareness training;

4.1.X Security incident management;

4.1.Y Server hardening; and

4.1.Z Workstation security.

4.2 Upon MD Anderson's request, Contractor will provide to MD Anderson: (i) all publicly releasable copies of Contractor's Information Security Policies and (ii) any other security documents Contractor maintains as indicated in Contractor's Information Security Policies.

5. **NETWORK ARCHITECTURE:**

5.1 Contractor will maintain network architecture that, at a minimum:

5.1.A Provides network topology diagram/design;

5.1.B Implements firewall protection on Contractor's network;

5.1.C Maintains routers and access control list (ACL);

5.1.D Provides network redundancy;

5.1.E Implements intrusion detection system/intrusion prevention system (IDS/IPS) technology;

5.1.F Provides demilitarized zone (DMZ) architecture for Internet systems;

5.1.G Maintains web applications that "face" the Internet on a server that is different from the server that contains a database or data with sensitive information;

5.1.H Provides enterprise virus protection;

5.1.I Maintains enterprise patch management;

5.1.J Provides dedicated customer servers or explains how this is accomplished in a secure virtual or segmented configuration;

5.1.K Provides remote access that is achieved over secure and encrypted connections;

5.1.L Maintains separate physical/logical testing environments;

5.1.M Provides the architectural software solution design with security controls as stated in this Rider; and

5.1.N Maintains a wireless network with controlled and secure access points.

6. **CONFIGURATIONS:**

6.1 Contractor will keep all of Contractor's computer systems used to provide services, directly or indirectly, to MD Anderson current with security patches and will take all steps necessary to protect such systems from malware. This requirement applies to: (i) the application code that makes up the application; (ii) the computer servers that host the applications' operating systems patch plan; (iii) all supporting software that is needed for the application to operate; and (iv) all database management systems that are used by the application.

6.2 Contractor will encrypt all sensitive information (PHI, student identifiable information, personnel information, intellectual property, etc.) for external or Internet transmissions that is configured with a strength of at least 128 bits.

6.3 For systems that support users, Contractor will have banners that display on those systems prior to access. These banners must notify users that: (i) the system is a business system; (ii) usage is monitored; and (iii) compliance is enforced.

6.4 For systems that support users, Contractor will only implement and use computers with password-protected screen savers that activate automatically to prevent unauthorized access when unattended.

6.5 Contractor will ensure that the computers Contractor uses to perform any work for MD Anderson do not include or access any software or services that are not necessary for Contractor's performance of such work. If Contractor is unable to comply with this requirement, then before Contractor may implement and use such computer Contractor must notify MD Anderson and provide a rationale satisfactory to MD Anderson, in MD Anderson's reasonable discretion, for Contractor's use of such computers.

6.6 All vendor-supplied default passwords or similar "published" access codes must be changed or disabled by Contractor for all installed operating systems, database management systems, network devices, application packages, and any other commercially-produced IT products.

6.7 Contractor will ensure that all passwords used by it or its employees, subcontractors, or other personnel must: (i) have a minimum of twelve (12) characters; (ii) expire upon a time period approved by MD Anderson; and (iii) have strength requirements approved by MD Anderson.

6.8 Contractor will ensure that all passwords used by it or its employees, subcontractors, or other personnel are never be stored in clear text or are easily decipherable.

6.9 Contractor will require all passwords for administrative accounts to: (i) have a minimum of fifteen (15) characters; (ii) expire upon a time period approved by MD Anderson; and (iii) have strength requirements approved by MD Anderson. If Contractor is unable to meet these password standards for administrative accounts, then Contractor must ensure that such administrative accounts use two-factor authentication. Contractor will ensure that all passwords for administrative accounts are never be stored in clear text or are easily decipherable.

7. OTHER CONFIGURATION REQUIREMENTS:

7.1 Contractor will check all systems and software to determine whether appropriate security settings are enabled.

7.2 Contractor will manage file and directory permissions for least privilege and need-to-know accesses.

7.3 Contractor will implement redundancy or high availability features for critical functions.

7.4 Contractor will authenticate all user access with either password, token, or biometrics.

7.5 All system changes will be approved, tested, and logged by Contractor.

7.6 Contractor will not use production data for testing unless the data has been declassified.

7.7 Contractor will implement application security that follows industry best practices (such as OWASP).

7.8 Contractor will implement an account lockout feature that is set for successive failed logon attempts for all systems that support users.

7.9 Contractor will prohibit split tunneling when connecting to customer networks.

8. PRODUCT DESIGN:

8.1 If Contractor provides any product that is used or provided in connection with any work for MD Anderson and that integrates with portable devices or stores sensitive information or information protected by law on portable devices, then Contractor will (i) encrypt all data that is stored on those

portable devices and (ii) implement and require secure password access to those portable devices and the information stored on them.

8.2 Contractor will ensure that access to any sensitive information or information protected by law that is conducted across a public connection is encrypted with a secured connection and requires user authentication.

8.3 All web-based applications will be regularly tested and monitored by Contractor for common application security vulnerabilities, and Contractor will ensure that the application server and database software technologies used are kept up to date with the latest security patches.

9. **ACCESS CONTROL:**

9.1 In the event of any termination, transfer, or change to job functions of any of Contractor's employees, subcontractors, or other personnel, Contractor must immediately remove or modify those persons' access to the products and services Contractor provides under this Agreement as necessary to ensure the security of those products and services.

9.2 Contractor will assign unique individual IDs and prohibit password sharing.

9.3 Contractor will ensure that critical data or systems are accessible by at least two (2) trusted and authorized individuals approved by MD Anderson.

9.4 Contractor will review all access permissions at least once annually and ensure that such reviews are updated as required for all server files, databases, programs, etc.

10. **MONITORING:**

10.1 Contractor will review access permissions according to regulatory requirements based on data content or at least annually for all server files, databases, programs, etc.

10.2 Contractor will implement system event logging on all servers and records who, what, and when access to such servers and records occurs.

10.3 Contractor will review and analyze system activities or accesses at least once every two (2) weeks.

10.4 Contractor will review system logs for failed logins or failed access attempts in compliance with at least the frequency required by regulatory requirements.

10.5 Contractor will periodically review logs for possible intrusion attempts and conducti such reviews at least according to regulatory requirements.

10.6 Contractor will review network and firewall logs on at least a bi-weekly basis.

10.7 Contractor will review and remove dormant accounts (i.e., one year of inactivity) on systems at least on a monthly basis.

10.8 Contractor will review wireless accesses on at least a monthly basis.

10.9 Contractor will perform scanning for rogue access points on at least a monthly basis.

10.10 Contractor will actively manage IDS/IPS systems and implements alert notifications.

10.11 Contractor will perform vulnerability scanning on at least a monthly basis.

10.12 Contractor will perform password complexity checking at least once every three (3) months.

11. **PHYSICAL SECURITY:**

11.1 Contractor will ensure that access to secure areas is controlled, including controls such as key distribution management, paper/electronic logs, or ensuring that a receptionist is always present when the doors to such areas are opened.

11.2 Contractor will (i) ensure that access to server rooms is controlled and (ii) follow need-to-know and least privilege concepts in controlling access to such rooms.

11.3 Contractor will ensure that all computer rooms have special safeguards in place (e.g., cipher locks, restricted access, room access log.)

11.4 Contractor will ensure that printed all Confidential Information or otherwise sensitive information is disposed of in a secure manner (e.g., shredded or otherwise destroyed securely).

11.5 Contractor will either (i) prohibit customer information (PHI, student data, social security numbers, Confidential Information, etc.) from being stored on laptop computers or other portable devices or (ii) only allow customer information to be stored on laptop computers or other portable devices if encrypted.

11.6 Contractor will ensure that all desktops that display Confidential Information or otherwise sensitive information are positioned to prevent unauthorized viewing of such information.

11.7 Contractor will require all visitors to be escorted in computer rooms or server areas.

11.8 Contractor will implement appropriate environmental controls where possible to manage equipment risks such as alarms, fire safety, cooling, heating, smoke detector, battery backup, etc.

11.9 Contractor will ensure that there are no external signs at its facilities indicating the content or value of the server room or any room containing Confidential Information or otherwise sensitive information.

11.10 Contractor will implement secure processes for destroying sensitive data on hard drives, tapes, or removable media, so that such data is no longer recoverable by any means once so destroyed.

12. **CONTINGENCY:**

12.1 Contractor will maintain and implement a written contingency plan for mission critical computing operations and provide a copy of such a plan to MD Anderson upon MD Anderson's request.

12.2 Contractor will maintain emergency procedures and responsibilities that are documented and stored securely at multiple sites.

12.3 Contractor will review, test, and update Contractor's contingency plan at least annually.

12.4 Contractor will identify which computing services must be provided within specified critical time frames in case of a disaster.

12.5 Contractor will identify cross-functional dependencies to determine how the failure in one system may negatively impact another one.

12.6 Contractor has and will maintain and implement written backup procedures and processes.

12.7 Contractor will periodically test the integrity of backup media.

12.8 Contractor will store backup media in a secure manner and ensure that access to such media is controlled.

12.9 Contractor will maintain a documented, tested, and updated disaster recovery plan and review such plan at least annually in collaboration with MD Anderson data owners.

12.10 Contractor will maintain off-site storage and document retrieval procedures for backups.

12.11 Contractor will provide rapid access to backup data.

12.12 Contractor will provide backup media that is appropriately labeled to avoid errors or data exposures.

13. **BUSINESS RELATIONSHIPS:**

13.1 Contractor will ensure that Contractor's employees, contractors, agents, and others sign confidentiality agreements before Contractor discloses proprietary and/or sensitive information to such employees, contractors, agents, and others.

13.2 Contractor will ensure that business associate agreements or other contracts that contain appropriate risk coverage provisions meeting the requirements of MD Anderson and Contractor's customers are in place before Contractor starts performance of work under this Agreement.

13.3 Contractor will ensure that Contractor's business associates are aware of MD Anderson's security policies and what is required of them under such policies.