Ascension Security Requirements Exhibit

In the event of a conflict between the terms in this Ascension Security Requirements Exhibit and the terms in the Agreement (other than this Ascension Security Requirements Exhibit) with respect to the subject matter of this Ascension Security Requirements Exhibit, the terms of the Agreement (other than this Ascension Security Requirements Exhibit) will control.

PURPOSE

This Exhibit defines the security requirements for Supplier when providing hardware, software, professional services, staffing services, or requiring software installation on Ascension Devices including Medical Devices. This includes but is not limited to Supplier when receiving, transmitting, accessing, and/or hosting Ascension Sensitive data or requiring access to Ascension Networks and/or performing business functions on behalf of or for Ascension.

DEFINITIONS

Application shall mean an executable software program, or group of programs, that is designed to deliver some or all of a series of steps needed to create, update, manage, calculate, or display information for a specific business purpose.

Ascension when used herein shall include Ascension and all Ascension Organizations.

Ascension Information shall mean all records and data, regardless of format, created, received, disclosed or used in the course of Ascension business or on Ascension time or Ascension systems, including, but not limited to, email, voicemail, text messages, paper documents, electronic documents and data, databases, application information, information on Ascension social media sites, such as Twitter and Facebook, Ascension intranet sites or external website postings, Ascension blog posts, or other electronic or photographic media. "Ascension Information" can include information maintained on a personal laptop, smartphone, cell phone, or mobile device, whether or not such device is connected to an Ascension system, including a Bring-Your-Own Device or "BYOD", if such information is created, received, or used in the course of Ascension business.

Ascension Organizations shall mean Ascension and all organizations directly or indirectly controlled by Ascension or its subsidiaries.

Availability shall mean the ability of an authorized person to use or access objects, resources, data, or information when needed, without undue delay.

Breach shall mean the circumvention or defeat of security controls which could result in a penetration of a system or network; or a violation of controls of a particular information system such that information assets or system components are susceptible to attacks which could adversely affect confidentiality, access, availability, and/or integrity of computer systems, components or data.

Business Associate shall mean an individual or organization who with respect to an Ascension Organization meets the definition of a business associate under HIPAA.

Business Associate Agreement shall mean a contract between a covered entity and a business associate meeting the requirements under HIPAA and entered into to ensure that the business associate will appropriately safeguard Protected Health Information. The Business Associate Agreement also serves to clarify and limit, as appropriate, the permissible uses and disclosures of Protected Health Information by the business associate, based on the relationship between the parties and the activities or services being performed by the business associate.

Cardholder Data shall mean the full personal account number from an individual's payment card as well as any of the following when combined with the full personal account number: cardholder name, expiration date and/or service code.

Confidentiality shall mean and include the property that data or information is not made available or disclosed to unauthorized persons or processes.

Cybersecurity is the art of protecting Networks, Devices, and data from unauthorized access or criminal use and the practice of ensuring Confidentiality, Integrity, and Availability of information.

Data Backup shall mean the process of copying all electronic data to media for applications and computer systems for recovery purposes.

Data Owner shall mean and include the individual(s) who has been designated to carry accountability for Ascension Organization data. Typically, the data owner makes the procedure and decisions for data, including identifying its sensitivity and criticality. (A Data Owner may also be a "System Owner".)

Device shall mean: (1) any piece of equipment used in computer input/output operations including but not limited to laptop computers, desktops, workstations, tablets, removable storage devices, card readers, servers, network components, printers, or any other mobile device; or (2) any medical device.

Disaster shall mean an unplanned event which results in a material and sustained loss of access to and use of the Supplier products or services resulting in the observed and material disruption or degradation on the processes of one or more of Supplier customers, excluding force majeure events. To avoid doubt, fire, flood, earthquake, wind, power outage, network outages (other than collapse of the Internet backbone), and catastrophic failure of Supplier's infrastructure are not force majeure events.

electronic Protected Health Information (ePHI) shall mean and include all individually identifiable health information that is created, received, transmitted or maintained in electronic form.

Encryption shall mean to modify or code data so that it is illegible without a specific key to decode it.

ePHI Application shall mean and include any application that creates, modifies, processes or stores electronic Protected Health Information.

Federated (SSO) System Federated identity management, also known as federated SSO, refers to the establishment of a trusted relationship between separate organizations and Supplier, such as application vendors or partners, allowing them to share identities and authenticate users across domains.

Firewall shall mean a device that prevents unauthorized access to private data, including ePHI.

HIPAA shall refer to the Health Insurance Portability and Accountability Act of 1996 and any amendments, regulations, rules, and guidance issued thereto and the relevant dates for compliance.

Integrity shall mean the property that data or information has not been altered or destroyed in an unauthorized manner.

Malicious Software shall mean the programs written and distributed with the intent to cause damage to or disrupt networks, systems, devices, servers and/or data, including, but not limited to viruses, worms, Trojan horses, and email bombs.

Medical Device shall mean any instrument, apparatus, appliance, material, or other article, whether used alone or in combination, together with any accessories or software for its proper functioning, intended by the manufacturer to be used for human beings in the:

1. Diagnosis, prevention, monitoring, treatment or alleviation of disease, injury, or handicap,
2. Investigation, replacement, or modification of the anatomy or of a physiological process,
3. and which does not achieve its principal intended action in or on the human body by pharmacological, immunological, or metabolic means, but which may be assisted in its function by such means. (Source: "Institute of Clinical Research")

Mobile Device shall mean and include any portable computer/device that allows for storing, accessing and organizing digital information. This includes, but is not limited to, iOS (Apple iPhone/iPad), Android, Windows Phone, and other smartphone, tablet, laptop computers, removable storage devices, and other mobile device units, with this capability.

Network shall mean a group of interconnected (via cable and/or wireless) computers and peripherals that is capable of sharing software and hardware resources between many users.

Offshore shall mean any geographic location outside of the United States.

Payment Cards shall mean, for purposes of Payment Card Industry Data Security Standard, any payment card/device that bears the logo of the founding members or strategic members of Payment Card Industry Security Standards Council. (American Express, Discover, MasterCard, JCB International, UnionPay and Visa).

Payment Card Industry Data Security Standard (PCI DSS) shall mean the requirements set forth for payment card data security throughout handling, processing, transmission, and storage.

Personally Identifiable Information (PII) shall mean any data that could potentially identify a specific individual.

Personal Data shall mean any data that is subject to Privacy Laws.

Physical Safeguards shall mean physical measures, policies, and procedures to protect an organization's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Policy shall mean high level statements that embrace Ascension's general beliefs, goals, objectives, and acceptable procedures for a specified subject area. Policies state required actions and may include pointers to standards. Policies require mandatory compliance.

Privacy Laws shall mean laws, states, regulations, rules, executive orders, directives, supervisory requirements in any jurisdictions worldwide, that relate to: (i) the confidentiality, collection, use, handling, processing, storage, security, protection, transfer or free movement of personal data, personally-identifiable information, customer information, or patient information; (ii) electronic data privacy; (iii) trans-border data flow; (iv) data protection; or (v) breach notification.

Procedures shall mean documented step-by-step instructions to accomplish specific tasks. Procedures may change frequently due to changes in systems, products, or business processes. Documented procedures help ensure that systems are implemented and maintained consistently across the organization. Procedures support standards in that they tell specifically how a standard will be implemented.

Public Network shall mean and include all systems, servers, routers, and lines not owned or controlled by Ascension Organizations that can be accessed through public access methods, including dial-up, DSL, ISDN, cable, wireless and other connection methods.

Risk shall mean the possibility of suffering harm or loss.

Security Event shall mean any observable occurrence in a system or network with a potential negative consequence.

Security Incident shall mean the unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

Sensitive shall mean and include all information containing anything deemed confidential by an Ascension Organization including ePHI, and Cardholder Data.

Server shall mean a computer that provides data to other computers. It may serve data to systems on a local area network (LAN) or a wide area network (WAN) over the Internet.

Single Sign-On (SSO) is an authentication method that allows users to access multiple applications or systems with a single set of login credentials.

Standards shall mean specific approaches, solutions, methodologies, products, or protocols that must be adhered to in the acquisition, deployment, implementation, retirement, disposal or use of systems or system components. Standards are intended to establish uniformity for information system infrastructures, applications, procedures, or data.

Supplier shall mean Ascension Organization's counterparty as set forth in the Agreement.

Supplier User shall mean and include the authorized individuals that routinely utilize Ascension information assets (i.e., applications, systems, networks and/or electronic data).

System Owner shall mean the individual(s) who has been designated to carry accountability for an Ascension information system. A system owner may also be a data owner. (See also "Data owner".)

Workstation shall mean any electronic computing device, for example, a desktop computer or laptop, or any other device that performs similar functions, and electronic media stored in its immediate environment.

Supplier Security Requirements

1. **General**
   - 1.1 Supplier must have an information security policy, with supporting Procedures in place that set forth how the Supplier will identify and manage its Cybersecurity Risks.
   - 1.2 Supplier must enter into an Ascension-approved contract with an Ascension Organization before a Supplier may connect to the Ascension Network.
   - 1.3 Supplier must have clearly established accountability and ownership of their Cybersecurity program. This should include assigned specific roles and responsibilities for the management along with proper staffing and financial resources.
   - 1.4 Supplier Users must be prohibited from making attempts to compromise or bypass Ascension security requirements.
   - 1.5 Background checks must be performed by a qualified Supplier prior to hiring all of its employees and subcontractors.

1.6 Supplier must have cyber Risk insurance coverage that provides financial mitigation to cyber-Risk incidents and impacts. The amounts of this coverage may be detailed in the agreement between the Ascension Organization and the Supplier.

1.7 Supplier must remain compatible with the most recent operating system version.

1.8 Supplier must immediately notify Ascension of employees or other personnel who were previously provided access to the Ascension Network or data and no longer need such access.

1.9 Supplier must follow a formal change management process.

1.10 Supplier must restrict the use of unauthorized software and hardware through written policy.

2. Acceptable Use

2.1 Supplier Users must protect the Confidentiality, Integrity, and Availability of Ascension Organization systems and data entrusted to them and restrict their activities to legitimate business purposes only.

2.2 Under no circumstance is a Supplier User authorized to use Ascension Organization Applications, systems, Networks, and/or electronic data for activities that are illegal under applicable local, state, federal or international law.

2.3 Individuals who are not Ascension associates and have been granted an email account are forbidden from using that email account to represent themselves as an Ascension associate.

3. Application and Data Security Controls

3.1 A current and periodic ongoing System and Organizational Controls ("SOC") 2 Type 2 report, a Health Information Trust Alliance Common Security Framework certification (HITRUST r2 certification), or a certified audit of ISO 27001 controls is required from all Supplier if Supplier processes or stores Ascension ePHI or other Personal Data or Sensitive data outside of the Ascension Network. The SOC 2, Type 2, HITRUST r2, or ISO 27001 certification requirement does not apply to disclosure of ePHI or Personal Data to governmental agencies, law enforcement, public health authorities and others when required by law.

If a cloud or hosting platform is leveraged by Supplier to store or process Ascension ePHI, other Personal Data or Sensitive data, in addition to the above requirement, a current SOC 2, Type 2 report, HITRUST r2 certification, or ISO 27001 certification is also required for the cloud or hosting platform.

3.1.1 SOC 2, Type 2 reports must be prepared by a Certified Public Accountant and performed in accordance with the American Institute of Certified Public Accountants Statement on Standards for Attestation Engagements No.18, and including in scope, at a minimum, the Security Trust Services Principle. Such reports must cover a six (6), nine (9), or twelve (12) month review period, be contiguous in nature (i.e., containing no time gaps in the period of time covered by subsequent reports) for the life of the contract between the Ascension Organization and Supplier and contain a favorable assessment of the Supplier's internal controls. Failure to provide the SOC2 Type 2 Reports as prescribed, or evidence of a material deficiency, shall be considered a material breach.

3.1.2 HITRUST r2 Certified Assessment Reports must be prepared by a HITRUST Assessor. On at least a biannual basis, a letter of certification is required with a supporting attestation report detailing the scope of the assessment, testing results and any corrective action plans. At a minimum, scope must include HIPAA Regulatory Risk Factors and other Risk factors as deemed appropriate through the Ascension Technologies assessment process. Such reports must be contiguous in nature (i.e., containing no time gaps in the period of time covered by subsequent reports) for the life of the contract between the Ascension Organization and Supplier and contain a favorable assessment of the Supplier's internal controls. Failure to provide the HITRUST r2 Certified Assessment Reports as prescribed, or evidence of a material deficiency, shall be considered a material breach.

3.1.3 ISO 27001 Certification Audit must be conducted by an ISO 27001 certified auditor. A Statement of Applicability (SoA) for ISO 27001 or ISO 27002 Information Security Controls Standard is required with a supporting attestation report detailing the scope and testing results of the audit. At a minimum, scope must include appropriate security controls to ensure HIPAA Regulatory compliance. Such reports must be contiguous in nature (i.e., containing no time gaps in the period of time covered by subsequent reports) for the life of the contract between the Ascension Organization and Supplier and contain a favorable assessment of the Supplier's internal controls. Failure to provide the ISO 27001 Reports as prescribed, or evidence of a material deficiency, shall be considered a material breach.

3.2 Ascension Personal Data, Sensitive data and other confidential or proprietary data may not be stored in any Offshore location and must remain within the 50 United States.

3.3 Offshore access to Ascension Network(s) and Personal Data, Sensitive data or other confidential or proprietary data (which includes, but is not limited to, data the Ascension Organization is required to protect under regulatory or legal requirements) is subject to the following limitations:

3.3.1 Data access may be allowed for support services such as help desk support, database support, troubleshooting, and pre-authorized critical business process support, and must meet the following criteria:

3.3.1.1 Offshore resources accessing Ascension data must be controlled by a technical platform that prevents downloading, printing, or exporting data to Devices located Offshore.

3.3.1.2 Offshore access permitted must be contractually documented, including the Offshore location, purpose, and the approved means of access.

4. Asset Security / Device and Media Control

4.1 Supplier, if storing Ascension data, must have a data destruction process in place which includes paper shredding and secure disposal for all electronic hardware. Prior to disposal or redeployment of electronic Devices, Medical Devices or media that contain ePHI, Personal Data or other Sensitive data, Supplier must ensure that such data cannot be recreated or recovered. Such erasure shall be in accordance with all applicable laws and the recommendations documented in Special Publication 800-88 (Guidelines for

Media Sanitation) of the National Institute of Standards and Technology, or its most recent publication providing guidelines for media sanitation. Final disposition of electronic and/or Medical Devices must be documented. All assets (including internal and external storage, data, etc.) belonging to Ascension must be returned upon termination of the contract between Supplier and the applicable Ascension Organization.

5. Audit Controls

5.1 Supplier solutions processing ePHI must have the capability to produce system and security logs in standard exportable format in near real time.

5.1.1 Supplier solutions must log and monitor events or actions which include, but are not limited to, logon attempts (including failed), changes to security settings and parameters, User account changes (e.g., added, changed privileges, deactivated, deleted), password resets, and system activity reviews of ePHI Applications as defined by HIPAA. Logs must be maintained for 12 months minimum.

5.1.2 These auditing mechanisms should record information such as the user identification associated with the event or actions, the program or command used to initiate the event or action and the time and date of the event or action.

5.2 Supplier must maintain a current enterprise-wide knowledge base of Supplier Users and its Devices, and Applications, including but not limited to software and hardware asset inventory, Network maps, Network utilization, and performance data.

6. Authorization and Access Management

6.1 Supplier must tightly control and manage the use of administrative privileges and limit the number of accounts that require administrative privilege. This includes removing administrative access from all Supplier Users unless there is a valid business need and established privileged identity access management controls.

6.2 Supplier must establish and maintain processes for secure Supplier User authentication protocols including:

6.2.1 A Federated (SSO) System is required between all separate organizations and Supplier if Supplier accesses Ascension Networks, systems, and Applications.

6.2.2 Within six (6) months of the effective date of Supplier's agreement with Customer, Supplier shall ensure its products and services are able to completely support Ascension's use of Single Sign-On (SSO) using modern authentication standards like SAML or OpenID/OAuth, specifically SSO user authentication standard with Ascension's Cloud based Federation Service which is Entra ID (formally Azure AD). For purposes of this Agreement, failure to abide by the foregoing shall be considered a material breach.

6.2.3 control of user IDs and other identifiers.

6.2.4 a secure method of assigning and selecting passwords.

6.2.5 use of unique identifier technologies.

6.2.6 blocking access to Supplier User identification after multiple unsuccessful attempts to gain access or the limitation placed on access for a particular system.

6.3 Supplier must apply strong authentication mechanisms to manage Supplier User identities and access including:

6.3.1 Multi-factor authentication technology to safeguard authentication attempts,

6.3.2 unique IDs (no shared IDs), and

6.3.3 an industry accepted password standard (for example, 90 day rotation, 12 characters, a history of 24 passwords, password complexity, etc.).

6.4 Supplier must limit access to Ascension Systems and data to authorized individuals with a valid business need.

7. **Business Associate Agreements**. Business Associate Agreements must be entered into between the applicable Ascension Organization and Supplier if Supplier meets the definition of a Business Associate.

8. **Confidentiality and Non - Disclosure Agreements.** Confidentiality or Non–Disclosure Agreements must be entered into between the applicable Ascension Organization and Supplier if Supplier creates, receives, accesses, maintains or transmits other, non-ePHI, Sensitive or proprietary data on behalf of Ascension Organizations. This requirement is met by entering into an agreement with Supplier that includes a Confidentiality obligation that would govern this scope.

9. **Contingency Operations.** Supplier must have an overall contingency plan and supporting Procedures for responding to an emergency that compromises the Confidentiality, Integrity and/or Availability of ePHI, Personal Data or other mission critical or Sensitive data contained in their environment. The contingency plan must include:

   9.1 Data Backup and recovery,

   9.2 Periodic impact analysis (e.g., business impact analysis or system criticality analysis),

   9.3 Disaster recovery plan,

   9.4 Emergency mode operation plan to enable continuation of critical business processes for protection of the security of ePHI, Personal Data or other mission critical, Sensitive, or proprietary data while operating in emergency mode,

   9.5 IT business continuity Procedures so person, patient, resident, and client care can be continued effectively in the event of emergency situations, addressing both external and internal Disasters, and

   9.6 Procedures for periodic testing and revision of the overall contingency plan.

10. **Data Backup and Storage.** Supplier, if hosting Ascension data, must establish and implement Procedures to create, maintain and verify exact copies of Ascension data, including but not limited to ePHI, Personal Data and Sensitive information, based on criteria including but not limited to patient care impact, government regulation, business operations and security best practices. Data custodians must ensure backup data is stored in a secure manner and must be available in the event of a system failure or other Disaster.

11. **Data Classification.** Security mechanisms for storage, transmission, handling, and destruction must be implemented to have a direct correlation with the Supplier's classification of the data. Supplier must implement appropriate security measures that correspond with the classification of the data when technically and operationally reasonable. Supplier is to provide its classification policy upon request.

12. **Facility Access Controls.** Supplier must have facility access controls that include but are not limited to: storage of all Servers and Network electronics in environmentally safe and secure

areas, maintenance of documented Standards and Procedures for gaining access, and maintenance of access controls and logs of access.

13. Incident Handling, Tracking and Response

13.1 Supplier must have documented Procedures for monitoring, analyzing and responding to Cybersecurity Incidents and reviewing the Cybersecurity Risks.

13.2 Supplier must have a notification policy for Breaches, Security Events and Security Incidents. Supplier must report Breaches and suspected or verified Security Events, Security Incidents or Policy violations to Ascension as promptly as possible, but in no event later than 5 days of discovery.

13.3 Supplier should share with Ascension any TTPs, IOCs or bad actor ids that have accessed and/or viewed Ascension data.

13.4 If Ascension Security or the applicable Ascension Organization notifies Supplier of a Breach, Security Event or Security Incident affecting the Ascension Network, then (1) Ascension Security or such Ascension Organization may require the Supplier to temporarily disconnect from the Ascension Network for an instructed period, in which case the Supplier will disconnect (and reconnect at the end of such period or in accordance with Section 13.5), or (2) the applicable Supplier may temporarily disconnect from the Ascension Network to the extent the Supplier reasonably determines that such disconnection is reasonably necessary to prevent or mitigate any material risk to the Supplier's Network or systems (a "Risk Determination").

13.5 If Supplier disconnects from the Ascension Network as a result of, or in connection with, any Breach, Security Event or Security Incident affecting the Ascension Network (whether or not such disconnection is authorized under this Exhibit or under any other agreement between an Ascension Organization and the Supplier), then, without limiting any other rights or remedies of the Ascension Organization in connection with such disconnection, the Supplier will reconnect to the Ascension Network: (1) if the Ascension Organization originally instructed the Supplier to disconnect from the Ascension Network, then upon the Ascension Organization's instruction and (2) if the Supplier disconnected from the Ascension Network as a result of a Risk Determination, then promptly upon the earlier of (A) the Supplier reasonably determining that any threat that such Breach, Security Event or Security Incident may pose to the Supplier that would arise from it reconnecting to the Ascension Network has been contained or adequately mitigated, or (B) an Ascension Organization delivering to the Supplier a written statement from a reasonable third-party vendor or contractor of Ascension Security or an Ascension Organization stating that the Breach, Security Event or Security Incident has been adequately contained and all compromised Ascension systems have either been brought offline or quarantined. The Supplier hereby expressly agrees that Mandiant (or its successors) is pre-approved by the Supplier for purposes of the foregoing.

14. Installation and Configuration

14.1 For all products requiring Ascension installation, all Transport Control Protocol (TCP) and User Datagram Protocol (UDP) ports and services not required for product use will be blocked prior to installation.

14.2 Supplier if installing products on the Ascension Network, must agree to change the IP address or Network configuration of a Device or system component at Ascension's request without charge.

14.3 All software and installation media not specifically required for the product, including files, scripts, messaging services and data will be removed from the product following installation.

15. Integrity. Supplier is required to protect ePHI from improper alteration or destruction. Ascension Technologies must approve any mechanism to be utilized to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

16. Malicious Software, Anti-Virus, and Encryption

16.1 Suppliers must implement the following security tools: endpoint protection, authentication, Firewall, antivirus, spam filtering, intrusion detection and prevention, Encryption, and Mobile Device Encryption.

16.2 Any Supplier-owned systems present on Ascension Networks (or Mobile Device used by Supplier attached to the platform or backup Devices), must have full disk Encryption and removable storage Encryption installed and enabled with an Ascension-approved Encryption solution.

16.3 Supplier supported electronic Devices (including business equipment and Medical Devices) must be protected with current security patches and approved endpoint protection solutions or be isolated from the Ascension Organization's Network.

16.4 Supplier must have a process to obtain, test and automatically deploy security patches and updates in a timely manner based on Risk. This process will confirm successful deployment and resolve update failures.

17. Perimeter Defense. Supplier must conduct regular internal and external vulnerability scans testing for client, Server, and Network infrastructure and implement processes to prevent, manage, mitigate, and remediate identified vulnerabilities.

18. Regulatory Compliance. Supplier must be able to demonstrate compliance with industry standards, all applicable Privacy Laws including HIPAA and any applicable Payment Card Industry Data Security Standards.

19. Remote Access

19.1 Establishing a remote connection to or through an Ascension Organization Network from a Public Network requires the use of an Ascension-approved secure remote access method. It is preferred that Supplier share pre-identified IP ranges from their homebase or leverage a B2B interface.

19.2 Any attempt to bypass or compromise information systems security Procedures is prohibited.

20. Risk Assessments. Supplier must have a process to conduct regular and comprehensive Cybersecurity Risk assessments. Results of the Cybersecurity Risk assessment as well as any action plans necessary to fully implement any required control points that have not yet been achieved shall be summarized and provided to Ascension.

21. **Security Awareness and Training.** Cybersecurity awareness and training must be provided by Supplier to all its employees and other personnel providing products or services to Ascension.

22. **Workstation Security.** Supplier, if processing Ascension data outside of the Ascension Network, must implement Physical Safeguards to restrict access to only authorized users. Workstations in areas that are vulnerable to theft must be protected using appropriate protection Procedures and anti-theft technologies.