Pursuant to the Master Agreement or other contract entered into between Supplier and Corewell to which these Supplier information security requirements are incorporated (the "**Agreement**"), Supplier's performance necessitates certain information security, cybersecurity, and risk management safeguards to ensure the security, confidentiality, integrity, and availability of Corewell data. As such, Supplier agrees to the following terms and conditions set forth in this Information Security Requirements Addendum to the Agreement (the "**Addendum**").

**Definitions**

Unless otherwise defined in this Addendum, capitalized terms used herein shall have the meaning given them in the Agreement.

"Corewell" means Corewell and its subsidiaries, affiliates, and successors.

"Supplier" means a vendor, contractor, supplier, or other entity who is providing goods and/or services to Corewell.

**Information Security Program**

**1.** Supplier shall be responsible for establishing, communicating and maintaining a written information security program with administrative, physical, technical and organizational safeguards related to securing and protecting Corewell Health, its systems, any deliverables, its data or information, including but not limited to all business information, confidential information, proprietary material and all personal data (whether of employees, contractors, consultants, customers, consumers, or other persons and whether in electronic or any other form or medium) that is accessed, collected, used, processed, stored, shared, distributed, transferred, disclosed, destroyed, or disposed of by Supplier ("**Data**" or "**Corewell Data**") that meets or exceeds Industry Best Practices (Industry Best Practice(s) means the degree of skill, care, foresight, standard of care, attention, diligence, expertise, knowledge, methods and operating practice reasonably and ordinarily expected of a leading supplier within the relevant industry), is reviewed and tested by management at least annually and is designed to: (i) ensure the security, integrity, availability and confidentiality of the Data; (ii) protect against any anticipated threats or hazards to the security or integrity of Data; (iii) protect against unauthorized access to or use of Data; (iv) ensure the proper disposal of Data; and, (v) comply with applicable state, federal and international laws and (vi) ensure that all Supplier personnel, consultants and vendors or authorized contractors / subcontractors comply with all of the foregoing. Upon Corewell Health's request, Supplier will provide Corewell a document outlining the security program required by this section.

**2.** Supplier reserves the right to update its policies and procedures and will provide notice of any significant changes to Corewell within 7 days of the effective date. Such changes will not materially degrade the security controls in effect at the time of the change.

**Governance, Risk Assessment and Management**

**1.** Supplier shall have a governance and risk management program that consists of policies, procedures, and technologies that address cybersecurity risks, threats and vulnerabilities that may negatively impact Corewell Data. Upon Corewell Health's request, Supplier will provide Corewell all relevant documents outlining its governance and risk management program.

**2.** Supplier will, at least annually, perform risk assessments that are designed to identify material threats (both internal and external) against Data, the likelihood of those threats occurring and the impact of those threats, to evaluate and analyze the appropriate level of information security safeguards ("**Risk**

**Assessments**"). Supplier's Risk Assessment process shall cover domains such as enterprise, third party, cloud, operational, technology, legal & regulatory risks, etc. Upon Corewell Health's request, Supplier will provide Corewell a report detailing the risk assessment, identified threats, and corrective action taken.

**3.** Supplier shall mitigate risk arising from subcontractors, cloud providers, and other service providers engaged by Supplier in the performance of the Services. Supplier remains fully responsible and liable for the acts, omissions, information security, regulatory compliance, and business continuity of all such parties as of performed by Supplier. Supplier shall ensure that all applicable contractual, information security, privacy, and continuity obligations under this agreement are contractually flown down to, and are enforceable against, such parties.

**Personnel Security**

**1.** Supplier shall perform identity proofing and background checks on all employees, contracted consultants and subcontractors, and will assess vendors ("**Users**") that will have access to Corewell Data, prior to employment or engagement. Any user who will have privileged access to Corewell Data must be identity proofed prior to gaining access.

**2.** Supplier shall immediately remove User's access rights from Supplier's systems, applications, servers, networks, and files utilized in the performance of its obligations under this Agreement. For purposes of this section, removal of access rights occurring within one (1) business day following the User's effective employment termination date shall be considered immediate.

**3.** Supplier shall have a formal security awareness and annual training program for all employees and contracted consultants that meets, or exceeds, the industry's best practices. Supplier shall perform periodic phishing simulations (≥ quarterly) with targeted retraining for clickers. **Supplier** will provide a high-level summary of the program and evidence of training to Corewell upon written request from Corewell Health.

**Physical and Environmental Security**

**1.** Supplier shall implement a comprehensive information system asset management program.

**2.** Supplier and its subcontractors shall have and implement access control policies and procedures for its facilities and data centers which shall be reviewed and modified as necessary but no less than annually.

**3.** Data centers used in the Supplier's performance under the Agreement shall be equipped and configured to assure continuous operation. The data centers should employ, at a minimum, uninterrupted power supply, redundant backup generators, smoke and heat alarm systems, water sensors, fire suppression systems, air conditioning and humidity controls, and ongoing monitoring.

**Disaster Recovery/Business Continuity**

**1.** Supplier shall maintain business continuity and disaster recovery plans for the purpose of ensuring the continued performance and high availability of Services. The disaster recovery and /or business continuity plan shall include (i) the identification of dependencies and critical functions (ii) processes and procedures for resumption of business operations, (iii) annual review by management and (iv) at least annual testing and validation of the program(s). Upon request from Corewell Health, **Supplier** will provide a copy of at least a high-level summary of the disaster recovery and/or business continuity plan and evidence of testing.

**Data Integrity**

**1.** Supplier must implement electronic mechanisms to corroborate that Corewell Data is accurate and reliable and not altered or destroyed in an unauthorized manner.

**2.** Supplier shall employ redundant techniques to ensure the integrity of the data on its servers and prevent data loss such as RAID, etc.

**3.** Supplier shall implement cryptographic mechanisms to protect information integrity such as cryptographic hash functions, digital signatures, checksums, message authentication codes, etc.

**4.** Supplier will ensure reasonable access to Data, including metadata and audit trails, by Corewell once a year, and regulatory authorities when requested, throughout the terms of the Agreement and any agreed upon post Agreement retention period.

**Data Security**

**1. Devices**

**a.** Supplier shall only store or process Corewell Data on/in assets owned or leased by Supplier, or Supplier contractors, or as agreed upon with Corewell in writing.

**b.** Supplier shall not store Corewell Data on storage devices including removable media such as flash drives, memory sticks, CDs, or DVDs.

**2. Mobile and Removable Media**

**a.** Supplier shall encrypt laptops, data storage devices, USB ports and devices and other mobile computing devices that may contain or access Corewell Data using an encryption algorithm that meets industry standards applicable to the provision of healthcare.

**b.** Supplier owned or BYOD mobile devices such as iPads/tablets, must utilize a containerized mobile device management solution to secure Data, access to Data, and prevent downloading and/or copying of Data to unmanaged devices.

**3. Data Transfers**

Supplier shall not store, process, or transfer Data outside United States.

**4. Offshore Services**

**a.** Supplier shall provide a list of offshore vendors or contractors/subcontractors ("**Offshore Vendor**") accessing Data upon written request from Corewell Health.

**b.** Supplier shall ensure that all Offshore Vendors follow Industry Best Practices to maintain the privacy and security of all Data to include controls such as:

i. Access is authorized, unique for each user, authenticated, and assigned with least and minimum necessary privileges, to include multi-factor authentication.

ii. Workstations and laptops must be hardened to Industry Best Practices, have Endpoint Detection and Response and configured to disable read and write

capabilities for all (i) local removable storage drives (including USB, zip, jazz, etc.,); (ii) print options; (iii) cut and paste and (iv) Boot alternative system.

iii. CCTV cameras will always record all access and egress to the secure room. Video shall be retained for at least 90 days.

iv. Layered security is enabled to ensure access to the economic zone, building and/or access to the facility is appropriate and managed.

v. Key card or biometric access must be required for entry to the secure room.

vi. Supplier's personnel will not have any access to personal mobile devices, personal email, instant messaging, or social media from within the secure room.

vii. A continuous/backed-up power source (e.g., Uninterrupted Power Supply and back-up generator) must be in place to supply power to, at a minimum, the facility, secure room, information technology infrastructure, CCTV system, and access control system.

**5. Media Sanitization / Disposal**

Supplier will follow the most current version of NIST SP800-88 Guidelines for media sanitization, and any successor standards, upon (i) retiring, replacing, or reassigning a device from which Data has been stored, processed or accessed and (ii) the physical destruction or secure deletion of hardcopy and electronic media that contained or stored Data.

**6. Encryption**

**a.** All Data in storage, at rest, backup media, email or in transit, shall be encrypted using a FIPS 140-3 compliant encryption algorithm and the encryption key stored separately from the media at all times. All transmissions, including email, shall enforce TLS v1.2 or higher (or successor), with modern cipher suites. Supplier shall decrypt Data as per industry standard mechanism.

**b.** Supplier must utilize a software-based cryptographic key management framework for both symmetric and asymmetric keys. All keys, both symmetric and asymmetric, must be specifically created for a single purpose.

**c.** Private/secret cryptographic keys must be stored within a valid key store.

**d.** The key recovery mechanism must not reduce the effective strength of encryption.

**e.** Key or data recovery must not be possible by any one individual

**f.** Archived keys and keying material must be stored in a manner and level of control that is equivalent with production key storage.

**g.** Any key found to be compromised must be revoked, destroyed or replaced as soon as feasible.

**h.** A trusted third-party certificate authority (CA) must be used to issue digital certificates and manage public keys and credentials for data encryption for any resources that are public-facing or hosted outside of Supplier's infrastructure.

For internal resources hosted entirely within Supplier's infrastructure or Supplier's private cloud tenant and not exposed to public networks, Supplier may utilize its own internally hosted certificate authority. The internal CA must be operated in accordance with Industry Best Practices and subject to appropriate administrative, technical, and physical controls, which may include:

i. Secure storage and access controls for root and intermediate CA keys.

ii. Regular audits and logging of certificate issuance and revocation activities.

iii. Automated certificate lifecycle management to ensure timely renewal and revocation.

iv. Compliance with applicable internal security policies and regulatory requirements.

All certificates, whether issued by a third-party or internal CA, must meet commercially acceptable minimum encryption standards.

**Technical Controls**

**1. Access Controls**

**Supplier** shall implement access controls that include but are not limited to the following:

**a.** Limit access to physical and logical assets and associated facilities to authorized users.

**b.** All access must be authorized, unique for each user, authenticated, and assigned with least and minimum necessary privileges, separation of duties. Interactive sessions shall terminate or lock after 15 minutes of inactivity for users accessing systems that store or process Corewell Data.

**c.** Password controls with Industry Best Practice password strength and complexity, expiration and history, removal of vendor supplied passwords, and account lockout. Any remote administrative support actions taken on a human account, require identity verification of the requestor.

**d.** Logical or physical controls to segregate Corewell Data from other customer data that is handled by the Supplier.

**e.** Privileged access users must use multi-factor authentication (MFA) for accessing systems and a different user identity for normal business use.

**f.** Access review of both general, administrative and privileged user accounts that occurs at least annually, documenting approvals and revocations.

**g.** Controls to identify and promptly locate all Supplier personnel and workstations with access to Data.

**h.** To the extent any biometric data is collected, stored, processed and/or used in the course of performing services for Corewell or Corewell users, Supplier represents and warrants that it is compliant with all applicable laws regulating biometric data, and Supplier further agrees to comply with all applicable laws related to biometric data including without limitation, providing required notices, performing required risk assessments, obtaining all required consents, allowing users to opt out and/or back in as required by law.

**2. Remote Access**

Supplier shall control access from external sources by using at minimum 2-factor authentication i.e., password and token.

**3. Network / Security Management**

**a.** To the extent Supplier leverages cloud, Supplier shall implement Industry Best Practices such as NIST, CISA, ISO, CSA STAR, etc.

**b.** Supplier shall protect network integrity by reasonable measures such as network segmentation, DDoS protections, etc.

**c.** Supplier shall have the ability to baseline and analyze network activity, detect anomalous activity and evaluate and respond to the potential impact of events.

**d.** Supplier shall ensure all unnecessary ports and protocols that are not being used for a business purpose are disabled (e.g., Remote Desktop Protocol [RDP] – Transmission Control Protocol [TCP] Port 3389).

**e.** Firewall/router filtering - Supplier shall maintain a network environment that utilizes firewalls to protect all ingress and egress points. Supplier shall house all public or internet facing applications in a DMZ that separates the publicly facing servers from the internal network.

**f.** Web Application Firewall (WAF) – Supplier shall implement WAF for internet facing services capable of preventing the exploitation of web application vulnerabilities covering at minimum OWASP's Top 10 web application security risks.

**g.** Protection against Malicious Code –

**i.** Supplier shall implement and maintain endpoint security controls that provide continuous monitoring, detection, and response to malicious or suspicious activity on all endpoints used to access, process, or store Customer Data. Such controls shall include behavior-based threat detection, centralized alerting, and the ability to investigate and contain security incidents in a timely manner. Endpoint protection technologies shall be kept current and appropriately managed, including having automatic updates enabled and using up to date virus signatures.

**ii.** Supplier shall implement filters at the email gateway to filter out emails with known malicious indicators and block suspicious Internet Protocol (IP) addresses at the firewall.

**iii.** Supplier shall use supported versions of operating systems and applications for which patches are actively deployed. All critical patches as defined by product owner and/or CVSS score shall be applied within 15 days of release.

**h.** IDS / IPS – Supplier shall utilize intrusion detection/intrusion prevention (IDS / IPS) systems to detect command and control activity and other potentially malicious activity that occurs across the network.

**i.** Supplier shall use application directory 'allowlisting' on all assets to ensure that only authorized software can run, and all unauthorized software is blocked from executing.

**j.** Wireless technology - Supplier shall implement a standard at least as stringent as the most current IEEE 802.11i standard when utilizing wireless technology to transmit Data or to access systems or Data.

**k.** Site Outage – Supplier will promptly place banners that report any site outages that will impact Supplier's ability to fulfill its obligations to Corewell and provide such notice via other direct methods such as email.

**l.** Vulnerability Scan - Supplier will conduct weekly vulnerability scans on varying internal and internet-facing systems, and will provide an attestation of those vulnerability scanning processes, frequencies, and remediation timelines to Corewell upon request.

**m.** Where practicable, Supplier shall disable or block legacy Server Message Block (SMB) protocols. In circumstances where disabling or blocking these protocols internally is not feasible due to operational requirements, the organization shall implement compensating controls designed to mitigate the identified risks and maintain an equivalent level of security.

**n.** Using an industry recognized third party, Supplier will perform no less than annually (i) web-application penetration tests on all applications that store, access, host, and process Data and (ii) internal and external network penetration tests of all systems and (iii) with an executive summary report and remediation plan issued by such third party and Supplier will provide an attestation of the frequency and process used for such testing to Corewell Health, upon request.

**o.** Remediation of identified vulnerabilities within the time set forth in the table below unless otherwise agreed to by Corewell in writing. Corewell may at any time request, and Supplier shall promptly provide, evidence of corrective action.

| **Severity (Based on CVSS scoring)** | **Corrective Action based on published date** |
|---|---|
| Critical or High | 15 / 30 calendar days |
| Medium | 90 calendar days |
| Low | 120 calendar days or as determined necessary based on risk |

## 4. System Hardening

Supplier shall implement policies and technical standards to harden its operating systems, networks, databases, and web services in compliance with laws and Industry Best Practice standards, including without limitation the Health Information Portability and Accountability Act (HIPAA), the Health

Information Technology for Economic and Clinical Health Act (HITECH), the Payment Card Industry Data Security Standards (PCI DSS), National Automated Clearinghouse Administration (NACHA), and the applicable National Institute of Standards and Technology (NIST) standards.

**5. Monitoring and Logging**

**a.** Supplier shall continuously monitor system integrity, security and performance to maintain needed resources and reduce the risk of unexpected downtime/system unavailability.

**b.** Supplier shall maintain audit logs of key events, systems, networks and applications including, but not limited to, logon attempts, account lockout, account administration and password resets, and remain in compliance with applicable laws and regulations. Upon Corewell Health's request, Supplier will provide access to the foregoing audit logs.

**c.** Supplier shall implement policies and procedures for continuous monitoring of information systems to detect and respond to cybersecurity events, and shall retain and adequately secure logs from both network devices and local hosts.

**6. Software/Hardware Development Life Cycle**

Supplier shall follow a documented Software/Hardware Life Cycle process that covers software design, development, implementation, and improvement. These practices shall include static and dynamic application security testing. The development/test and production environments shall be logically separated. All development and testing must be performed in a development / test environment. Where production data is replicated or utilized in non-production environments (including development, testing, and staging) and where sensitive data cannot be de-identified or masked, such environments shall implement security and privacy controls equivalent to those applied in production. This includes, but is not limited to, access controls, encryption, monitoring, and data protection measures, or other compensating controls to mitigate risks associated with exposure of sensitive information.

**7. Change Management**

**a.** Supplier shall implement documented change management and problem management processes which require management review and approval of any production system and software environment changes.

**8. Artificial Intelligence and Machine Learning Capabilities "AI System"**

**a.** Supplier shall not use, and shall not permit any third party to use, any Data or information provided by or on behalf of Corewell Health, including any Corewell Confidential Information , to develop, train, re-train, validate, fine tune, optimize, or improve any of Supplier's or any third party's AI Technology artificial intelligence algorithm, model, system, or technology, including any generative artificial intelligence, machine learning, predictive artificial intelligence, retrieval augmented generation, or large language model technology (collectively, "**AI Technology**") solely for itself or for the benefit of any other person or entity, without Corewell Health's prior written authorization, which may be withheld or withdrawn at Corewell Health's sole discretion. Except as set forth above, Corewell or its third parties may use AI to provide services to Corewell as outlined in this agreement.

**b.** Supplier shall establish and implement a risk management system that identifies and evaluates the risks that may emerge when the AI System is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse.

**c.** If Corewell approves the use of their data for development of AI as set forth in 8(a), the Supplier shall ensure the data sets used in the development of the AI System, shall be subject to appropriate data governance and management practices including but not limited to (i) training, validation and testing; (ii) data collection; (iii) relevant assumptions, with respect to the information that the data are supposed to measure and represent (iv) examination in view of possible biases and avoidance of bias; (v) the identification of any possible data gaps or limitations, and how those gaps and limitations can be addressed.

**d.** Supplier shall ensure the AI System includes appropriate disclosures related to processing of personal information under applicable data privacy laws.

**e.** Supplier shall, upon request, provide Corewell with appropriate disclosures so that Corewell may pass along to Data Subjects with respect to a description of the AI System.

**f.** Supplier shall ensure the AI System automatically records and monitors event logs while the AI System is operating.

**g.** Supplier shall ensure the AI System is designed and developed in such a way, including with appropriate human-machine interface tools, that it can be effectively overseen by natural persons.

**h.** Supplier shall ensure that the AI System will comply with Industry Best Practices and applicable laws and regulations.

**i.** Supplier shall, upon Corewell's request, provide written attestation and architectural documentation demonstrating compliance with the requirements of this Section 8.

**9. Backup and Recovery**

a) Supplier will maintain a backup of Data and shall ensure Services are promptly recovered and available within a commercially reasonable timeframe not to exceed 24 hours in the event of a disruption or interruption.

b) If using physical hardware for backup, Supplier shall store a backup of Data or replicated copy of the backup in an off-site reputable facility no less than daily.

c) Supplier shall test backup and recovery plans not less than once annually.

**Cybersecurity Incident Response**

**1.** Supplier shall execute and maintain a Cybersecurity Incident Response Plan (CSIRP) that is supported by a cross-functional response and recovery team that are on call 24x7, 365 days a year. Upon Corewell's request, Supplier will provide its CSIRP to Corewell for review.

**2.** "**Cybersecurity Incident**" means: (a) the actual unauthorized acquisition, access, use, processing, alteration, ransom, loss or disclosure of Data, information systems or network; (b) a reasonable suspicion or the reasonable belief that there has been an unauthorized acquisition, access, use, processing, alteration,

loss, or disclosure of Data or information systems supporting Data or Supplier authentication credentials, or (c) any other event which results in the inability to use an applicable system or Data, unauthorized access or disclosure of Data or information. This does not include trivial incidents that occur on a daily basis, such as unsuccessful scans, "pings" or unsuccessful attempts to penetrate computer networks or servers maintained by Supplier.

**3.** Supplier must determine a Cybersecurity Incident without unreasonable delay following discovery and must: (a) notify Corewell within 48 hours of awareness of a successful Cybersecurity Incident that is impacting Data or services provided to Corewell as required by this agreement, by email to threatresponse@corewellhealth.org; and (b) take all reasonable steps to mitigate and remediate the Cybersecurity Incident and minimize impact to Data, systems that host, store, process or transmit Corewell Data and/or systems that are used in connection with the services under the Agreement (c) provide Corewell with information detailing the cause of the Cybersecurity Incident, the impact of the Cybersecurity Incident on Data, the corrective actions taken to resolve the Cybersecurity Incident, actions taken to prevent future Cybersecurity Incidents (d) furnish timely preliminary, interim and final incident reports to Corewell with all relevant investigative details, including identification, containment, eradication, recovery, a comprehensive outline detailing specifics of the exposed Data and lessons learned and (e) reasonably cooperate with Corewell Health.

**4.** If Supplier fails to mitigate or remediate a successful Cybersecurity Incident that directly poses an active, ongoing risk to Corewell Data within a commercially reasonable time period, such failure will constitute a material breach of the Agreement.

**Security Breaches**

**1.** "**Security Breach**" means (i) any act or omission that materially compromises either the security, confidentiality or integrity of Data or the physical, technical, administrative or organizational safeguards put in place by Supplier that relate to the protection of the security, confidentiality or integrity of Data or (ii) receipt of a complaint in relation to the privacy practices of Supplier or a breach or alleged breach of this Agreement relating to such privacy practices.

**2.** Supplier represents and warrants that its collection, access, use, storage, disposal and disclosure of Data does and will comply with all applicable federal, state, and foreign privacy, security and data protection laws, as well as all other applicable regulations and directives.

**3.** In the event that Supplier becomes aware of a Security Breach, Supplier shall notify Corewell Information Security of the circumstances and scope of the breach within 48 Hours of awareness. All notifications will be made to threatresponse@corewellhealth.org. Supplier will (i) investigate the cause(s) of the breach, (ii) ensure that mitigating and/or remedial measures are reasonably instituted to prevent further breaches, (iii) provide a detailed summary of Data impacted by the breach and (iv) upon request will provide Corewell a copy of the Data impacted, and will reasonably cooperate with Corewell in addressing the Security Breach, mitigating any associated harm caused by the Security Beach and meeting all legal requirements associated with such breaches. Supplier shall be responsible for its and Corewell Health's reasonable costs associated with meeting the requirements of the Security Breach law, including costs associated with issuing notifications to individuals and government agencies where applicable.

**4.** With regard to Security Breaches involving PHI Data as defined in 45 CFR 160.103, in the event of a conflict between the terms of this Appendix and the terms of the Business Associate Agreement, the terms of the Business Associate Agreement will prevail.

**Auditing and Downstream Suppliers**

**1. Auditing**

**a.** No less than annually and in compliance with applicable laws, Supplier shall conduct an independent third-party audit of its information security program e.g., SSAE 18, SOC 1, SOC 2, NIST, ISO 27001-2013, HITRUST, EHNAC, etc. and provide a copy of the report upon request by Corewell Health.

**b.** Corewell shall have the right, at its own expense, during normal business hours and with thirty (30) days' reasonable written advance notice, to audit, evaluate, assess, and review Supplier's policies, controls and security posture to ensure compliance with the terms and conditions of this Agreement, via a reasonable security questionnaire, policies, controls, and third party audit reports. Corewell shall have the right to conduct such audit by use of its own employees and internal audit staff, or by use of outside consultants and auditors. In the event of a Cybersecurity Incident, Corewell has only to provide five business (5) days' notice of the intent to audit. Supplier agrees to complete, within a reasonable period of time not to exceed 30 business days, the security questionnaire provided by Corewell regarding Supplier's information security and privacy programs. Supplier shall consider any suggested safeguards as identified by Corewell during the information security program audit questionnaire. In the event Supplier opts to not remediate suggested safeguards, Corewell reserves the right to terminate in accordance with the terms of this Agreement.

**2. Downstream Service Providers**

**a.** Supplier must perform an initial due diligence review and an annual reassessment of downstream service providers (e.g., third party service providers, subcontractor) that may have access to Corewell Data. These reviews will validate that such downstream service providers have information security controls, including cybersecurity controls, similar to and no less protective of Data than the requirements in this Appendix and the Agreement. Upon request from Corewell Health, Supplier shall make available a summary of its due diligence for such downstream service providers.

**b.** Supplier shall ensure that contracts are in place with any Supplier subcontractor who stores, processes, transmits or accesses Data in connection with the Agreement such that they are obligated to comply with restrictions and controls substantially similar to those applicable to Supplier under the terms of this Appendix B.

**Return / Destruction of Data**

Upon the termination or expiration of the Agreement, or at any other time upon the written request of Corewell Health, Supplier will promptly return to Corewell or destroy all Data in Supplier's possession or control, together with all copies, summaries and analyses, regardless of the format in which the information exists or is stored. In case of destruction, Supplier upon request will promptly send a written certification that destruction has been accomplished. However, subject to applicable laws, Supplier is entitled to retain the Data for the sole purpose of determining its obligations under this Agreement. With regard to Data stored electronically on backup tapes, servers or other electronic media, the parties agree to make reasonable efforts to destroy such Data without undue expense or business interruption; however, Data stored is subject to the obligations of confidentiality and non-use contained in this Appendix and the Agreement for as long as it is stored. The foregoing obligations shall not apply to such Data or data of individuals to the extent the Supplier is required to retain such Data for a longer period in accordance with any laws or regulations

or delete such data in accordance with any laws or regulations. Upon expiration of any such requirement, Supplier shall destroy such Data as per the terms in this Appendix.

**Cybersecurity Insurance**

**1.** Supplier agrees to purchase and maintain throughout the term of the Agreement technology/professional liability insurance policy, covering liabilities for any and all loss resulting or arising from, directly or indirectly, acts, errors, or omissions, in rendering or failure in rendering technology/professional services or in connection with the specific services described in this Agreement.

**2.** Supplier agrees to purchase and maintain throughout the term of the Agreement a network security and privacy liability insurance policy (commonly referred to as a Cyb er Liability insurance policy), covering claims, incidents, events and the like, arising from, based upon or in any way related to: Violation or infringement of any right of privacy, including breach of security and breach of security/privacy laws, rules or regulations globally, now or hereinafter constituted or amended; Data theft, damage, unauthorized disclosure, destruction, or corruption, including without limitation, unauthorized access, unauthorized use, identity theft, theft of personally identifiable information or confidential corporate information in whatever form, transmission of a computer virus or other type of malicious code inclusive of ransomware or extortion-ware, among others; and participation in a denial of service attack on third party computer systems; Loss or denial of service; for liability related to any alleged infringement of copyright, trademark, trade dress, service mark, plagiarism, misappropriation or theft of ideas, defamation, libel, slander, invasion of the right of privacy; with a minimum limit of $5,000,000 each and every claim and in the aggregate. Such coverage must include privacy and security liability, privacy regulatory defense and payment of civil fines and penalties, payment of credit card provider penalties, fines and costs. Such insurance must explicitly address all of the foregoing without limitation if caused by an employee of Supplier or an independent contractor working on behalf of Supplier in performing services under this Agreement. Policy must provide coverage for wrongful acts, claims, and lawsuits anywhere in the world.

**3.** Supplier further agrees to keep and maintain said insurance coverage in full force and effect during the term of the Agreement and continue the coverage (or purchase “tail coverage”) which will extend the reporting period for incidents arising out of or related to the Agreement for at least three (3) years beyond the termination of the Agreement.