The purpose of this Security Requirements Exhibit is to specify **Service Provider**'s information security, cybersecurity and risk management responsibilities to ensure security, confidentiality, integrity and availability of the Data. Any capitalized terms used herein have the meaning ascribed to such terms as set forth in the Agreement or this Exhibit.

A. Information Security Program

Service Provider 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 Quest Diagnostics, 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 **Service Provider** (**"Data" or "Quest Diagnostics Data"**) that meets or exceeds best practice accepted standards, 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 **Service Provider** personnel, consultants and vendors or authorized contractors / subcontractors comply with all of the foregoing.

B. Governance, Risk Assessment and Management

Service Provider 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 Quest Diagnostics Data.

Service Provider 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"). Service Provider's Risk Assessment process shall cover domains such as enterprise, third party, cloud, operational, technology, legal & regulatory risks, etc.

C. Personnel Security

1. **Service Provider** shall perform background checks on all employees, consultants and vendors or contractors / subcontractors ("**Users**") that will have access to Quest Diagnostics Data, prior to employment or engagement.

2. **Service Provider** shall sign a Quest Diagnostics Access Agreement before access is granted to Quest Diagnostics' network, systems, or applications.

3. **Service Provider** shall remove User's access rights from **Service Provider's** systems, applications, servers, networks, and files utilized in the performance of its obligations under this Agreement within the earlier of (i) one business day following the User's effective employment termination date; (ii) a reasonable period (not to exceed three (3) business days) after the User's role no longer required access; or (iii) after a defined period of inactivity of a User, which shall be no greater than ninety (90) days.

4. **Service Provider** shall maintain a list of Users with access to Quest Diagnostics systems and will provide a copy of this list to Quest Diagnostics upon its request. **Service Provider** shall notify Quest Diagnostics within a reasonable timeframe, not to exceed two (2) business days, when a user no longer requires access, so that Quest Diagnostics may disable their access to Quest Diagnostics systems.

5. **Service Provider** shall have a formal security awareness and annual training program for all employees, consultants and partners that includes such topics but are not limited to social engineering, phishing, incident management, ransomware, etc, **Service Provider** will provide a copy of the program and evidence of training to Quest Diagnostics upon request.

D. Physical and Environmental Security

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

2. **Service Provider** 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 semi-annually.

3. Data centers used in the **Service Provider'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.

E. Disaster Recovery/Business Continuity

Service Provider shall maintain business continuity and disaster recovery plans for cloud and on premises, the purpose of ensuring the continued performance of Services and recoverability of Data. The disaster recovery and /or business continuity plan shall include (i) the identification of dependencies and critical functions (ii) process and procedure for determination and isolation or disconnection of systems that were impacted, triaging impacted systems for restoration and recovery (ii) processes and procedures for recovery of Data and resumption of business operations, (iii) annual review by management and (iv) at least annual testing and validation of the program(s). Upon request from Quest Diagnostics, **Service Provider** will provide a copy of at least a high-level summary of the disaster recovery and/or business continuity plan and evidence of testing.

F. Data Integrity

1. **Service Provider** must implement electronic mechanisms to corroborate that Quest Diagnostics Data is accurate and reliable and not altered or destroyed in an unauthorized manner.

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

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

4. **Service Provider** will ensure timely access to Data, including metadata and audit trails, by Quest Diagnostics and regulatory authorities throughout the terms of the Agreement and any agreed upon post Agreement retention period.

G. Data Security

1. Devices

- **a.** **Service Provider** shall only store or process Quest Diagnostics Data on /in assets owned or leased by **Service Provider**, or **Service Provider** contractors, or as agreed upon with Quest Diagnostics.
- **b.** **Service Provider** shall not store Quest Diagnostics Data on storage devices including removable media such as flash drives, memory sticks, CDs, or DVDs.

2. Mobile and Removable Media

- **a.** **Service Provider** shall encrypt laptops, data storage devices, USB ports and devices and other mobile computing devices that may contain or access Quest Diagnostics Data using an encryption algorithm that meets industry standards applicable to the provision of healthcare.
- **b.** **Service Provider** owned or BYOD mobile devices such as iPads/tablets, must utilize a containerized mobile device management solution to secure Data or access to Data.

3. Data Transfers

Service Provider shall not access, store, process, transmit or transfer Data outside United States.

4. Offshore Services

- **a.** **Service Provider** shall not engage an offshore vendor or contractors /subcontractors ("Offshore Vendor") without the prior written approval of Quest Diagnostics.
- **b.** In the event Quest Diagnostics approves the use of an Offshore Vendor for any portion of the Services, **Service Provider** shall ensure that the following protections are in place:
  - **i.** never access, store, process or transfer Data outside United States.
  - **ii.** Access is authorized, unique for each user, authenticated, and assigned with least and minimum necessary privileges, to include multi-factor authentication.
  - **iii.** Workstations and laptops must be hardened to best practice standards, have anti-malware protection/detection programs with signatures kept up to date 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.

iv. With respect to any **Service Provider** facility located outside of the United States from which there may be contact with any Data, or privileged or administrative access to Data in a production environment, the secure room must, in addition to other requirements under this Security Requirements Exhibit, meet the following :

- Facility must be physically and logically separate from other entities that may occupy the building.
- Key card or biometric access must be required for entry to the secure room.
- Service Provider's personnel will not have any access to personal mobile devices, personal email, instant messaging, or social media from within the secure room.
- 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

Service Provider 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. Service Provider shall decrypt Data as per industry standard mechanism.

b. Service Provider must utilize a hardware-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. A trusted third-party certificate authority must be used to issue digital certificates and manage the public keys and credentials for data encryption.

H. Technical Controls

1. Access Controls

Service Provider 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 and includes session timeout not to exceed 15 minutes.

c. Password controls with best practice password strength and complexity, expiration and history, removal of vendor supplied passwords, and account lockout.

d. Logical or physical controls to segregate Quest Diagnostics Data from other customer data that is handled by the **Service Provider**.

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

f. MFA for all access for email and accounts that access applications exposed to the Internet, where sensitive Data or Quest Diagnostics Data is stored, accessed, processed or transmitted and for all privileged account access,

g. Access review of both general, administrative and privileged user accounts that occurs at least semi-annually.

h. To the extent any biometric data is collected, stored, processed and/or used in the course of performing services for Quest Diagnostics or Quest Diagnostics users, **Service Provider** represents and warrants that it is compliant

with all laws regulating biometric data, and **Service Provider** 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

a. **Service Provider** shall control access from external sources by using minimum 2-factor authentication i.e., password and token.

b. **Service Provider** shall follow Quest Diagnostics' remote access procedures when accessing Quest Diagnostics network. If **Service Provider** personnel have access to Quest Diagnostics internal network and systems, they will follow all applicable Quest Diagnostics policies and procedures identified by Quest Diagnostics.

3. Network / Security Management

a. Develop and regularly update a comprehensive network diagram that describes systems and data flows within Service Provider's network

b. To the extent **Service Provider** leverages cloud, **Service Provider** shall implement best practices such as NIST, CISA, CSA STAR, etc.

c. **Service Provider** shall protect network integrity by reasonable measures such as network segmentation, etc.

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

e. **Service Provider** shall only use licensed and supported RDP or other remote desktop services.

f. Service Provider 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).

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

h. Protection against Malicious Code –

i. **Service Provider** shall implement automated tools to detect, prevent, remove and remedy malicious code on desktops, servers, e-mail and internet access. **Service Provider** shall ensure antivirus and anti-malware software and signatures are up to date and automatic updates are enabled.

ii. **Service Provider** 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. **Service Provider** shall use supported versions of operating systems 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.

i. IDS / IPS – **Service Provider** 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.

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

k. Wireless technology - **Service Provider** 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.

l. Site Outage – **Service Provider** will promptly report to Quest Diagnostics any site outages that will impact **Service Provider**'s ability to fulfill its obligations to Quest Diagnostics.

m. Vulnerability Scan - **Service Provider** will conduct a weekly vulnerability scan on all internal and internet-facing systems. An executive summary report will be provided to Quest Diagnostics upon request.

n. **Service Provider** will disable or block Server Message Block (SMB) protocol outbound and remove or disable outdated versions of SMB. Using an industry recognized third party, **Service Provider** will perform no less than annually (i) web-application penetration test on all applications that store, access, host, process Data (ii) internal and external network penetration test of all systems and (iii) with an executive summary report issued by such third party and provided to Quest Diagnostics upon request.

o. Remediation of identified vulnerabilities within the time set forth in the table below unless otherwise agreed to by Quest Diagnostics in writing. Quest Diagnostics may at any time request, and **Service Provider** 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

Service Provider shall implement policies and technical standards to harden its operating systems, networks, databases, and web services in compliance with laws and 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)) and the applicable National Institute of Standards and Technology (NIST) standards.

5. Monitoring and Logging

a. **Service Provider** shall continuously monitor system integrity, security and performance to maintain needed resources and reduce the risk of unexpected downtime/system unavailability.
b. **Service Provider** 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 retain in compliance with applicable laws and regulations.
c. **Service Provider** shall implement policies and procedures for monitoring security logs on a regular basis and shall retain and adequately secure logs from both network devices and local hosts.

6. Software/Hardware Development Life Cycle

Service Provider shall follow a documented Software/Hardware Life Cycle process that covers software design, development, and improvement. The development/test and production environments shall be physically separated. All development and testing must be performed in a development / test environment. Sensitive production Data shall not be used for testing purposes, unless de-identified, using applicable regulatory and best practice standards.

7. Change Management

a. **Service Provider** shall implement documented change management and problem management processes which require management review and approval of any production system and software environment changes.
b. **Change Notifications**. In addition to any specific requirements and subject to any specific conditions set forth in this Security Requirements Exhibit or the Agreement (including any applicable Statements of Work), **Service Provider** shall provide Quest with at least sixty (60) days' prior written notice of any changes that effect **Service Provider**'s obligations under this Security Requirements Exhibit or the Agreement.

8. Software Security

If **Service Provider** is developing software and/or hosting software for Quest Diagnostics and/or deploying software on Quest Diagnostics network, **Service Provider** shall comply with the following controls:

a. **Service Provider** shall ensure secure coding practices are followed so that software provided or utilized under the Agreement is not vulnerable to known exploits and no open-source or public domain software is used unless approved by Quest Diagnostics.
b. **Service Provider** shall comply with Quest Diagnostics technical security requirements to be defined as part of the development life cycle process for applications developed specifically for Quest Diagnostics and will reside on the Quest Diagnostics' network.
c. **Service Provider**, prior to production, will perform network and application vulnerability and penetration testing of the application and/or web service using industry-recognized third-party tools or vendors.
d. **Service Provider** will provide to Quest Diagnostics a written report of the results of the pre-production vulnerability and/or penetration scans and tests.
e. **Service Provider** at no cost to Quest Diagnostics will remediate all vulnerabilities prior to implementation of the application/web service.
f. **Service Provider** or project team will provide security documentation created throughout the development process. The documentation will include, at a minimum, the security requirements, design documentation and diagram, implementation, and test results.

g. **Service Provider** shall ensure all resources on the development team will be trained in secure code practices.

h. For applications developed on behalf of Quest Diagnostics, **Service Provider** will use a source code control system that authenticates and audits all changes to the code and related configuration.

i. **Service Provider's** deliverables shall not be considered accepted by Quest Diagnostics until the security requirements are completed, documentation received, and all security issues have been resolved.

j. **Service Provider**, at no additional cost, will perform post-production network vulnerability scans and application penetration tests at least annually as or required by applicable law or regulation using industry recognized network and application third party tools or vendors.

k. **Service Provider** will follow, at a minimum the Open Web Application Security Project (OWASP) Testing Guide, including the OWASP top 10 list of vulnerabilities, when scanning software applications and networks.

l. **Service Provider** must perform both authenticated and non-authenticated application scans and manual verification of vulnerabilities identified in those scans.

m. If **Service Provider** uses a third-party contractor to develop, scan and/or host applications that process, store and/or manage Quest Diagnostics Data, the obligations of this Exhibit shall apply to **Service Provider's** contractor.

n. Any significant architectural change will require additional penetration testing and the entirety of this section will be re-evaluated by **Service Provider** and appropriate documentation reflecting such re-evaluation will be provided to Quest Diagnostics.

9. Artificial Intelligence and Machine Learning Capabilities "AI System"

a. **Service Provider** shall not use, and shall not permit any third party to use, any Data or information provided by or on behalf of Quest Diagnostics, including any Quest Confidential Information ("Data"), to develop, train, re-train, validate, fine tune, optimize, update, improve, or modify any of **Service Provider'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") for itself or for the benefit of any other person or entity, without Quest Diagnostic's prior written authorization, which may be withheld or withdrawn at Quest's sole discretion

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

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

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

g. **Service Provider** 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. **Service Provider** shall ensure that the AI System will comply with best practice standards and applicable laws and regulations.

i. **Service Provider** shall provide reasonable notice to Quest Diagnostics when Artificial Intelligence and Machine Learning Capabilities are introduced into existing services and products.

10. Backup and Recovery

a) **Service Provider** will maintain a backup of Data and shall ensure Services are promptly recovered and available within 24 hours in the event of a disruption, interruption or Cybersecurity Incident.

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

c) **Service Provider** shall test backup plan not less than once annually**.**

I. Cybersecurity Incident Response

1. **Service Provider** shall execute and maintain a Cybersecurity Incident Response Plan (CSIRP) that is supported by a cross-functional response and recovery team and such CSIRP shall include response and notification procedures for a ransomware incident.

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 suspicious 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 **Service Provider** 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 attempts to penetrate computer networks or servers maintained by **Service Provider**.

3. **Service Provider** must determine a Cybersecurity Incident without unreasonable delay following discovery and must: (a) notify Quest Diagnostics within forty-eight (48) hours of awareness of a Cybersecurity Incident by email to ITSecurityIncidentReporting@questdiagnostics.com; and (b) take all reasonable steps to detect, analyze, mitigate and remediate the Cybersecurity Incident and minimize impact to Data, systems that host, store, process or transmit Quest Diagnostics Data and/or systems that are used in connection with the services under the Agreement (c) provide Quest Diagnostics 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 Quest Diagnostics with all relevant investigative details, including identification, containment, eradication, recovery, a comprehensive outline detailing specifics of the exposed Data and lessons learned and (e) cooperate fully with Quest Diagnostics.

4. If Service Provider fails to detect, analyze, mitigate or remediate a Cybersecurity Incident within a commercially reasonable time period, such failure may be deemed by Quest Diagnostics to be a material breach of the Agreement. Quest Diagnostics may immediately suspend **Service Provider's** access to Quest Diagnostics systems and Data without cost or penalty upon notification of a Cybersecurity Incident. **Service Provider** shall not be relieved of its obligation to continue to provide the Services under the Agreement, except to the extent such Services are directly impacted by the termination of access, and (b) **Service Provider's** Fees shall be equitably reduced to reflect the Services that are no longer being provided (until access is restored, if such access is restored).

J. Security Breaches

"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 **Service Provider** 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 **Service Provider** or a breach or alleged breach of this Agreement relating to such privacy practices.

Service Provider 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.

In the event that **Service Provider** has a suspected or confirmed Security Breach, **Service Provider** shall notify Quest Diagnostics IT Security of the circumstances and scope of the breach within forty-eight (48) hours of awareness. All notifications will be made to ITSecurityIncidentReporting@questdiagnostics.com. **Service Provider** will (i) investigate the cause(s) of the breach, (ii) ensure that mitigating and/or remedial measures are immediately instituted to prevent further breaches, (iii) provide a detailed summary of Data impacted by the breach and (iv) upon request will provide Quest Diagnostics a copy of the Data impacted, and will fully and reasonably cooperate with Quest Diagnostics in addressing the Security Breach, mitigating any associated harm caused by the Security Beach and meeting all legal requirements associated with such breaches. **Service Provider** shall be responsible for its and Quest Diagnostics' 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.

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 Exhibit and the terms of the Business Associate Agreement, the terms of the Business Associate Agreement will prevail.

K. Auditing and Downstream Service Providers

1. Auditing

a. No less than annually and in compliance with applicable laws, **Service Provider** shall conduct an independent third-party audit of its information security program e.g., SSAE 18, SOC 2, NIST, ISO 27001-2013, HITRUST, EHNAC, etc. and provide a copy of the report upon request by Quest Diagnostics. To the extent **Service Provider** processes credit cards on behalf of Quest Diagnostics, **Service Provider** will provide a copy of a PCI-QSA issued Attestation of Compliance (AOC) annually and maintain PCI compliance for the duration of the Agreement. **Service Provider** will notify Quest Diagnostics at any time during the Agreement if they are no longer PCI compliant and will provide a plan outlining efforts to remediate.

b. Quest Diagnostics shall have the right, at its own expense, during normal business hours and with 30 days' reasonable written advance notice, to evaluate, test, assess, and review **Service Provider's** facilities, books, records, policies, controls and systems to ensure compliance with the terms and conditions of this Agreement. Quest Diagnostics 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, Quest Diagnostics has only to provide 5 days' notice of the intent to audit. In addition, Quest Diagnostics, in its sole determination, may request a security questionnaire in lieu of an on-site audit. **Service Provider** agrees to complete, within fourteen (14) days of receipt, the security questionnaire provided by Quest Diagnostics regarding **Service Provider's** information security and privacy programs. **Service Provider** shall implement any required safeguards as identified by Quest Diagnostics during the information security program audit, system testing or from the security assessment questionnaire.

c. Service Provider represents and warrants that the information and documentation provided to Quest Diagnostics in security questionnaires, assessments or audits is and shall be true and accurate.

2. Downstream Service Providers

a. **Service Provider** must perform a due diligence review at least once every calendar year of any downstream service providers (e.g., third party service providers, subcontractor) that may have access to Quest Diagnostics Data. The review will validate the downstream service providers have information security controls, including cybersecurity controls, similar to and no less protective of Data than the requirements in this Exhibit and the Agreement. Upon request from Quest Diagnostics, **Service Provider** shall make available a summary of its due diligence for such downstream service providers.

b. **Service Provider** shall ensure the applicable provisions of the Agreement and this Exhibit are incorporated into contracts in place with any **Service Provider** subcontractor who stores, processes, transmits or accesses Data in connection with the Agreement such that they are obligated to comply with the terms set forth in this Exhibit.

L. Return / Destruction of Data

Upon the termination or expiration of the Agreement, or at any other time upon the written request of Quest Diagnostics, **Service Provider** will within 30 days of request promptly return to Quest Diagnostics or destroy all Data in **Service Provider'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, **Service Provider** upon request will promptly send a written certification that destruction has been accomplished. However, subject to applicable laws, **Service Provider** is entitled to retain one copy of 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 Exhibit 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 **Service Provider** 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, **Service Provider** shall destroy such Data as per the terms in this Exhibit.

M. Cybersecurity Insurance

Service Provider 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.

Service Provider agrees to purchase and maintain throughout the term of the Agreement a network security and privacy liability insurance policy (commonly referred to as a Cyber 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 **Service Provider** or an independent contractor working on behalf of **Service Provider** in performing services under this Agreement. Policy must provide coverage for wrongful acts, claims, and lawsuits anywhere in the world.

Service Provider 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.