EXHIBIT A – INFORMATION SECURITY AGREEMENT

1. Definitions. For purposes of this ISA, the following definitions shall apply:

1.1. "Business Associate" means Vendor acting as a Business Associate as such term is defined in 45 C. F. R. 160.103.

1.2. "Customer" means Humana.

1.3. "Computer Security Incident" or "Incident" as defined in the National Institute of Standards and Technology (NIST) special publication (SP) 800-61 rev.2 means a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

1.4. Unless otherwise defined in the Agreement, "Customer Confidential Information" means:

1.4.1. trade secrets, all past, present and future business activities and all information related to the business of Customer, its parent company and its subsidiaries and affiliated companies and its or their clients, members and/or enrollees, that is provided to Vendor or its technology infrastructure partners through the performance of Services (as defined in the Agreement and available on Customer's mainframe, networks, LANs and workstations and all software, middleware, firmware, groupware and licensed internal code whether owned or licensed currently or in the future by Customer and accessed by Vendor or any of Vendor's employees, contingent workers and subcontractors (such Vendor employees, contingent workers and subcontractors collectively referenced hereinafter as "Representatives") by any direct or remote access method and also including, but not limited to, any information relating to the pricing, software or technical information, hardware, methods, processes, financial data, compilations, lists, apparatus, statistics, program, research, development or related information of Customer, its subsidiaries or affiliated companies or its clients, patients, members and/or enrollees concerning past, present or future business activities of said entities, and/or the results of any analysis of any of the foregoing and outcome of any provision of services by Vendor and Representatives under this Agreement, provided that disclosure of the foregoing in response, and only to such extent and for such purpose, to a valid order by a court of competent jurisdiction or as otherwise required by law shall not be considered a breach of Vendor's duty under this ISA to hold Customer Confidential Information in strict confidence.

1.4.2. Customer Confidential Information does not include information that:

1.4.2.1. has been previously published or is now or becomes public knowledge through no fault or negligence of Vendor or Representatives; or

1.4.2.2. can be established by documentary evidence to have been made available to Vendor or Representatives, without restriction on disclosure, by a third party not under obligation of confidentiality with respect to the disclosed information; or

1.4.2.3. can be established by documentary evidence to have been independently developed by Vendor or Representatives.

1.5. "Customer Information Systems" means information systems resources supplied and operated by or on behalf of Customer, including but not limited to, network infrastructure, computer systems, workstations, laptops, hardware, software, databases, storage media, proprietary applications, printers, and internet connectivity that are owned, controlled, or administered by Customer.

1.6. "Information Security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

1.7. "Multi-Function Device" or "MFD" means an office machine which incorporates the functionality of multiple devices in one. A typical MFD may provide a combination of some or all of the following services:

1.7.1. Printing

1.7.2. Scanning

1.7.3. Photocopying

1.7.4. Faxing

1.7.5. Emailing

i.1.8. Intentionally Omitted

1.9. "Personal Computer" or "PC" means any laptop, notebook, desktop, netbook, or any other personal computing apparatus or device which is used to access, process, or display information. This definition does not include computing devices operating as servers in a hardened, controlled access, secured data center.

ii.1.10. Intentionally Omitted

1.11. "Security Breach" means the unauthorized acquisition, access, use, or disclosure of information which compromises the security or privacy of such information, except where an unauthorized person, to whom such information is disclosed, would not reasonably have been able to retain such information. Security Breach does not include:

1.11.1. Any unintentional acquisition, access, or use of Customer Confidential Information by an employee or individual acting under the authority of Vendor if:

1.11.1.1. such acquisition, access or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with Vendor; and

1.11.1.2. such information is not further acquired, accessed, used, or disclosed by any person; or

1.11.2. Any inadvertent disclosure from an individual who is otherwise authorized to access Customer Confidential Information at a facility operated by Vendor to another similarly situated individual at the same facility; and

1.11.3. Any such information received as a result of such disclosure is not further acquired, accessed, used or disclosed without authorization by any person.

1.12. "Vendor Representative" means an employee, contractor, or agent of Vendor, or of its subcontractors, who provide Services to Customer.

1.13. "Vendor Processing Resources" means information processing resources supplied or operated by Vendor, including without limitation, network infrastructure, computer systems, workstations, laptops, hardware, software, databases, storage media, printers, proprietary applications,

Internet connectivity, printers and hard copies which are used, either directly or indirectly, in support of Vendor processing.

2. Provisions applicable for all Vendors

2.1. General Requirements

2.1.1. Vendor shall not collect or generate metadata related to Customer or its members for any purpose other than to provide the services for which the Vendor has been engaged by Customer.

2.1.2. Unless previously authorized by Customer in writing, all work performed by Vendor related to the Agreement shall be performed from the secured Vendor Facilities located at the Vendor location(s) designated in the Agreement and/or relevant statement of work(s).

2.1.3. Vendor shall only have access to Customer Information Systems authorized by Customer and shall use such access solely for providing Services to Customer. Vendor shall not attempt to access any applications, systems, or data which Customer has not authorized Vendor to access, nor shall Vendor use access credentials to create automated processes except as authorized in a fully executed statement of work. If authorized, Vendor shall access and use such applications, data, and systems only as minimally necessary to provide Services to Customer and solely for such purposes. Vendor's attempt to access any applications, data, or systems in violation of the terms in this Section shall be a material breach of the Agreement.

2.1.4. Although the security and confidentiality requirements specified herein are minimum standards intended to facilitate the protection of Customer Confidential Information, it remains Vendor's responsibility to take appropriate additional measures and precautions necessary to ensure the confidentiality, availability, and integrity of Customer Confidential Information.

2.2. Information Security Policies

2.2.1. Vendor shall have a security control framework based upon an accepted standard governing the information security within Vendor's industry (e.g., NIST, HiTrust, ISO, etc.). Such framework shall utilize a standard set of controls, and shall be meant to include, but not be limited to, commercially available and widespread use of precautionary measures.

2.2.2. Vendor shall develop and maintain a comprehensive Information Security Policy ("Policy").

2.2.3. Vendor shall review the Policy not less than annually and whenever there is a material change in practices.

2.2.4. Vendor shall have a designated employee or group of employees who shall maintain said Policy.

2.2.5. Vendor shall monitor its Policy to ensure that the program described therein is operating in a manner reasonably calculated to prevent unauthorized access.

2.3. Physical Security

2.3.1. Vendor shall maintain appropriate physical security controls (including facility and environmental controls) to prevent unauthorized physical access to Vendor Processing Resources and areas in which Customer Confidential Information is stored or processed. Where practicable, this obligation shall include controls to physically protect hardware (e.g., lockdown devices).

2.3.2. Vendor shall adopt and implement a written facility security plan which documents such controls and the policies and procedures through which such controls will be maintained.

2.3.3. Vendor shall maintain appropriate records of maintenance performed on Vendor Processing Resources and on the physical control mechanisms used to secure Vendor Processing Resources.

2.3.4. Vendor shall notify Customer before moving storage or processing of Customer Confidential Information or changing the location of a Vendor facility where services are being provided to any location not previously authorized by Customer.

2.3.5. Vendor shall restrict entry to Vendor's area(s) where Customer Confidential Information is stored, accessed, or processed solely to Vendor's Representatives with a need to access such area(s) and information and escorted guests.

2.3.6. Vendor shall implement reasonable best practices for infrastructure systems including, but not limited to, fire extinguishing, cooling, and emergency systems designed to reasonably ensure employee safety.

2.3.7. Vendor shall provide physical entry controls for all areas where Customer Confidential Information is stored, accessed, or processed that are commensurate with the sensitivity of the Customer Confidential Information; each of Vendor's Representatives accessing these areas must employ one or more unique, individually identifiable entry controls (such as card keys) that provide an audit trail of each entry. All visitors who enter these areas must be logged and escorted by one of Vendor's Representatives who are authorized to access such area.

2.3.8. Vendor shall regularly monitor areas where Customer Confidential Information is handled, stored, and/or processed through the use of appropriate measures such as cameras, guards, and entry logs.

2.3.9. In situations where a statement of work allows work to be conducted outside of an authorized facility, Vendors shall implement and maintain a set of policies and procedures which provide guidance and instruction on protecting information outside the office.

2.4. Risk Management

2.4.1. Vendor shall develop and use a defined risk assessment methodology.

2.4.2. Vendor shall conduct risk assessments and reviews upon significant change and in no case less than once per year.

2.4.3. Vendor will document results of all risk assessments, develop action plans for the mitigation of findings, and track the progress of such action plans.

2.5. Configuration and Change Management

2.5.1. Vendor shall define and control a formal, documented configuration management policy. Said policy shall address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

2.5.2. Vendor shall review and update as needed, but in no case shall such reviews occur less than annually.

2.5.3. Vendor shall ensure that all changes to systems are documented and follow recognized

change control procedures.

2.5.4. Vendor shall ensure that segregation of duties exists such that the individual or system performing changes is not the same individual or system which approves such changes.

2.6. Third Party Management

2.6.1. **Intentionally Removed.**

2.6.2. Unless specifically authorized and agreed to by the parties in a statement of work under the Agreement, Vendor shall not provide or allow access to Customer Confidential Information by any third party.

2.6.3. Vendor shall conduct risk assessments and reviews upon all third Parties with access to Customer Confidential Information no less than once per year. A summary of such assessment methodology along with a summary of results shall be provided to Customer upon written request and prior approval by said Third Parties which will not be unreasonably withheld.

2.6.4. Vendor shall be responsible for ensuring that all downstream partners that have access to Customer Confidential Information are in full compliance with the terms of this ISA.

2.6.5. Vendor shall report to Customer, upon written request and upon any material change, the names and locations of all downstream partners with access to Customer Confidential Information, and the nature of the services provided by those partners that necessitates access to Customer Confidential Information. Vendor shall further report to Customer a consolidated list of the names and all locations of all downstream partners with access to Customer Confidential Information, and the nature of the services provided by those partners that necessitates access to Customer Confidential Information annually.

2.7. Mobile Device Security

2.7.1. Vendor shall ensure that appropriate measures for securing portable devices are explained and followed by all employees, this includes, but is not limited to, any time the device is not in a secured office location (e.g., in automobiles, on aircraft, at home, etc.).

2.7.2. Vendor shall create and maintain policies and standards which provide guidance on transporting and securing devices which may contain Customer Confidential Information when outside the office.

2.8. Encryption Requirements

2.8.1. Vendor shall utilize dedicated encryption keys. All encryption keys used to protect Customer Confidential Information shall be uniquely associated to Customer. The use of said encryption keys to encrypt non-Customer data is forbidden.

2.8.2. All keys will be protected against modification; secret and private keys need to be protected against unauthorized disclosure.

2.8.3. FIPS-approved or NIST-recommended cryptographic algorithms commensurate with key size shall be used whenever cryptographic services are applied.

2.8.4. Vendor shall implement full-disk encryption on any built-in or removable storage media in any Vendor-controlled portable computer which may access, store, transmit, or process Customer Confidential Information. All such encryption shall minimally meet the Advanced Encryption Standard with a 256-bit cypher key (“AES256”) as outlined in the Federal Information Processing Standards publication 197. (“FIPS197”)

2.8.5. Vendor shall ensure that all passwords are transmitted securely and encrypted when in storage. In the event that a hashing algorithm is used, Vendor must use a randomly-generated salt.

2.8.6. Plaintext Encryption and/or Decryption keys must be adequately secured. Only those trusted associates who have a "need to know" should be given access to the key or security environment storing keys. Storage of these keys must be separate and distinct from the encrypted data.

2.8.7. Intentionally Deleted.

2.8.8. When a cryptographic key is compromised, all use of the key to apply cryptographic protection to information (e.g., compute a digital signature or encrypt information) shall cease, and the compromised key shall be revoked. However, the continued use of the key under controlled circumstances to remove or verify the protections (e.g., decrypt or verify a digital signature) may be warranted. All compromised keys must be retired and replaced in a timely fashion.

2.8.9. Vendor encryption key management systems should be designed so that the compromise of a single key compromises as little data as possible and avoids having a catastrophic weakness.

2.8.10. Vendor should have a compromise-recovery plan for restoring cryptographic security services in the event of a key compromise.

2.8.11. Encryption keys will not persist unencrypted in any environment beyond the minimum time required for use. To the maximum extent operationally possible, plaintext symmetric and private keys are restricted to physically protected containers. This includes key generators, key-transport devices, key loaders, cryptographic modules, and key-storage devices.

2.8.12. Encryption key metadata is used to identify attributes, parameters, or the intended use of a key, and as such contains the key's control information. This information requires elevated protection commensurate with Key Management System ("KMS") access.

2.8.13. Vendors will use an accountability system that keeps track of each access to symmetric and private keys in plaintext form.

2.8.14. In the event that tapes are used for system backup, such tapes shall be encrypted and appropriately inventoried and logged as to location and planned destruction date.

2.9. Remote Computing Requirements

All permitted and authorized remote sessions that may entail access to Customer Confidential Information shall only be performed via a secure Virtual Private Network ("VPN").

2.10. Malware Protection

Vendor shall install, enable and keep current reputable, commercially available anti-malware software on all Vendor servers and Personal Computers used in accessing, processing, transmitting, or storing Customer Confidential Information.

2.11. Password, Access and Identity Management

2.11.1. Vendor shall require that all Vendor Representatives with access to Customer Confidential Information use a unique username and password (collectively "Login

Credentials"). Password shall expire no less often than every ninety (90) days. Said password shall be at minimum 8 characters in length, include at least three of the following: alpha, numeric, special character, and case sensitivity. Additionally, said password shall not contain any portion of username, shall change every ninety (90) days maximum, and not be reused for a minimum of 365 days.

2.11.2. Vendor shall ensure that Login Credentials are terminated in a timely manner upon the removal of Vendor Representatives from provision of the Services for any reason.

2.11.3. Vendor shall use unique logins on all network equipment whenever commercially possible.

2.11.4. Vendor shall not allow the sharing of passwords.

2.11.5. Vendor shall not allow the use of vendor-supplied default credentials.

2.11.6. Vendor shall review access log files for indications of credentials, including but not limited to, sharing of credentials, sharing of passwords, etc.

2.11.7. Vendor shall review access log files for suspicious login activity. Any such identified activity shall be promptly investigated and appropriately mitigated.

2.12. Logical/System Access Control and Monitoring

2.12.1. Vendor shall implement a formal user registration and de-registration procedure for granting and revoking access to Vendor Processing Resources; and upon termination of any of Vendor Representative (including any contingent worker), Vendor shall ensure that such Vendor Representative's access to Customer Confidential Information is revoked and notification to Customer is made no later than one business day following termination. In the event of an involuntary termination, Vendor shall ensure all access is revoked immediately.

2.12.2. Vendor shall maintain appropriate access control mechanisms to prevent all access to Customer Information Systems and/or Vendor Processing Resources, except by (a) specified users expressly authorized by Customer and (b) Vendor Representatives who have a "need to access" to perform a particular function in support of Vendor Processing.

2.12.3. Vendor shall maintain appropriate mechanisms and processes for detecting, recording, analyzing, and resolving unauthorized attempts to access Customer Information Systems or Vendor Processing Resources.

2.12.4. Vendor shall review access logs not less than quarterly to ensure that access permissions are appropriate and necessary.

2.12.5. Vendor's operating-system security mechanisms must be configured to support appropriate security procedures, and should at a minimum:

2.12.5.1. Identify and verify the identity of each authorized user; and

2.12.5.2. Record successful and failed system accesses

2.12.6. Vendor shall ensure that segregation of duties exists such that the individual or system granting access is not the same individual or system which approves such access.

2.13. Cloud Computing

2.13.1. Vendor shall ensure that all Customer Confidential Information stored in any cloud based solution be encrypted per all aforementioned encryption requirements.

2.13.2. Customer Confidential Information shall be protected by a unique Data Encryption Key ("DEK") that must not be stored in plaintext. Master Key Encryption Keys ("KEK"), preferably those provided by Humana, will be used to decrypt subordinate DEK's. All KEK's regardless of source must be stored in a Federal Information Processing Standards ("FIPS") 140 certified KMS Hardware Security Module ("HSM") under split knowledge access controls. Vendor will retain exclusive control of keys and not provide subsequent access to any other entity. Vendors shall ensure a unique KEK is used for DEK's specific to Humana confidential information. Any use of a Humana specific KEK or subordinate DEK for other than Human information and purposes is strictly forbidden.

2.14. Configuration and Change Management

2.14.1. Vendor shall define and control a formal, documented configuration management policy. Said policy shall address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Vendor shall review said policy and update as needed but in no case shall such reviews occur less than annually.

2.14.2. Vendor shall ensure that all changes to systems follow recognized change control procedures.

2.15. Vulnerability Management and Patching

2.15.1. Vendor shall adhere to applicable standards governing the patch management criticality rankings and patching time frame requirements for all systems including, but not limited to, switches, routers, appliances, servers, and workstation PC's.

2.15.2. Vendor shall conduct comprehensive scans for known vulnerabilities on all externally facing systems, managed and controlled by Vendor, in line with Vendor's scanning standards.

2.15.3. Vendor shall conduct comprehensive scans for known vulnerabilities on the Vendor managed and controlled network, in line with Vendor's scanning standards.

2.15.4. All critical and high vulnerabilities must be remediated within the Vendor recognized vulnerability management standard. Should such preclusion exist, mitigating controls offering the same level of protection must be implemented within the aforementioned timeframe.

2.15.5. Vendor shall ensure that all urgent, critical, and high patches are implemented in a timely manner. Urgent and critical patches must be implemented within the Vendor recognized patch management standard, unless application requirements preclude such patching. Should such preclusion exist, mitigating controls offering the same level of protection must be implemented within the aforementioned timeframe.

2.16. Secure Disposal

All media containing Customer Confidential Information shall be disposed of via appropriate physical destruction (e.g., shredding, drilling, crushing, incinerating, etc.).

2.17. Vendor Representative Training and Related Matters

2.17.1. At Customer's specific request and per the terms of the Agreement, Vendor shall perform criminal background checks on any Vendor Representative with potential access to Customer Confidential Information. Such background checks must be performed prior to allowing such individual to access Customer Confidential Information; and Vendor shall

not allow any individual who does not have a satisfactory background check to access Customer Confidential Information.

iii.2.17.2. Intentionally Omitted.

2.17.3 For any Vendor Representatives who have access to Customer Confidential Information outside the United States, such background checks shall include a nationwide criminal background check.

2.17.4 Vendor shall train new Vendor Representatives (including contingent workers) on the acceptable use and handling of Customer Confidential Information.

2.17.5 Vendor shall provide periodic and mandatory Information Security training and awareness to its Vendor Representatives. Such training shall occur not less than annually.

iv.2.18. Audit

2.18.1. Not more than once per calendar year, Customer reserves the right, upon reasonable notice and at Customer's expense, to review said vendor risk program. This right includes the use of Customer personnel or may be delegated to a third party.

2.18.2. In the event of a Computer Security Incident or Security Breach, the calendar limitation listed above is not applicable.

2.18.3. Humana reserves the right to audit compliance with the subject matter covered within this ISA on an annual basis, onsite at Vendor location. This right includes the use of Customer personnel or may be delegated to a third party.

2.19. Network Controls

2.19.1. Vendor shall implement appropriate controls to ensure that only authorized devices are provisioned network access when physically connected to the network.

2.19.2. As necessary, Vendor shall provision logically or physically segregated network to allow guest access for visitors to their facilities. In no case shall vendor allow guests or other non-Vendor managed and controlled personnel access to the production networks.

2.19.3. Vendor shall implement technical controls to filter inappropriate and unnecessary web content including, but not limited to, pornography, gambling, violence, webmail, social media, etc.

2.19.4. All Vendor-controlled wireless connections shall be secured utilizing Wi-Fi Protected Access 2 ("WPA2") or better security protocol.

2.19.5. Vendor shall ensure that interconnections within Vendor, with other companies, and with the Internet ("Access Points"), whether wired or wireless, into the Vendor network are protected by using firewalls, secure tunnels, and/or access lists on routers.

2.19.6. Vendor shall ensure that a network management system is used to monitor its local network and servers. Thresholds and alarms shall be established to notify Vendor of potential problems or outages.

2.19.7. Vendor shall implement either host-based or network-based Intrusion Detection Solution ("IDS") or Intrusion Protection Solution ("IPS") on any Vendor controlled network used to

process, store, transmit, or access Customer Confidential Information. Appropriate response and recovery plans to monitor potential unauthorized access to said network and systems shall be implemented.

2.19.8. Vendor shall implement a Data Loss Prevention system ("DLP") to prevent the accidental or intentional distribution of Customer Confidential Information.

2.19.9. Vendor shall secure all unused network ports.

2.20. Transmission Protection

2.20.1. Vendor shall encrypt all data, records, and files containing Customer Confidential Information that shall be transmitted wirelessly or travel across public networks.

2.20.2. Intentionally Omitted.

2.21. Incident and Breach Response

2.21.1. Vendor shall report each Computer Security Incident or Security Breach to Customer in an appropriate and timely manner.

2.21.2. Vendor shall establish formal incident response policies and procedures.

2.21.3. Vendor shall establish formal documented management responsibilities and procedures to ensure a timely, effective, and orderly response to information Computer Security Incidents or Security Breaches.

2.21.4. Vendor shall identify appropriate resources to monitor the internal environment for security events, to evaluate security events, and to respond to incidents in a timely manner.

2.21.5. In the event of a Computer Security Incident or Security Breach, Vendor shall collect, retain, and present evidence in support of potential legal action in accordance with the rules for evidence in the relevant jurisdiction.

2.21.6. Vendor shall, if requested, provide applicable information, including but not limited to, forensic copies, network and activity logs, and reasonable access to Vendor Representatives to assist Customer in investigating the incident.

2.22. Security Contact

2.22.1. Vendor shall assign an individual to act as the primary security liaison between Vendor and Customer (the "Security Custodian"). This person shall be a trusted source at Vendor for the distribution of passwords and other confidential security matters.

3. Provisions applicable to all Business Associate Vendors. In addition to section 2 above, the provisions in this section are applicable to all Vendors who access, store, process, transmit, or are otherwise exposed to PHI.

INTENTIONALLY DELETED. Vendor will not be permitted to access, store, transmit, or otherwise be exposed to PHI.

4. Provisions applicable to Vendors who handle PCI DSS covered data – In addition to section 2 above, the provisions in this section are applicable to Vendors who handle or process cardholder data.

INTENTIONALLY DELETED. Vendor will not be permitted to handle PCI DSS covered data.

5. Provisions applicable to Vendors who are providing services that include a Mobile Application ("Mobile App") to Humana.

INTENTIONALLY DELETED. Vendor will not be permitted to provide services that include a Mobile Application.

6. Provisions applicable to Vendors who will have Humana software ("Customer Provided Software") installed on Vendor equipment.

INTENTIONALLY DELETED. Vendor is not permitted to have Humana software installed on Vendor equipment.

7. Section reserved for customized service requirements (e.g., identified deficiencies which need remediation)