**ADDENDUM**

**THIS ADDENDUM (“Addendum”)** effective \_\_\_\_\_\_\_, 20\_\_ (“Effective Date”) to the \_\_\_\_\_\_\_\_\_\_\_\_ between Health Care Service Corporation, a Mutual Legal Reserve Company (“HCSC”) and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (“VENDOR”) dated \_\_\_\_, 20\_\_ (“Agreement”) contains additional terms governing the Minimum Security Requirements to which VENDOR shall adhere to in the course of business with HCSC.

For and in consideration of the mutual premises and covenants contained therein and herein, the adequacy of which is acknowledged by the parties, the underlying agreement between the parties is modified and amended to include the following terms:

**MINIMUM SECURITY REQUIREMENTS**

1. **Security of HCSC Data**: At all times, VENDOR shall use appropriate controls, as required by current State or Federal regulation(s) and requirements expressed here within to secure HCSC data to prevent loss and unauthorized access or disclosure. In the event that VENDOR handles payment card data, VENDOR shall be Payment Card Industry (PCI) compliant.
2. **Security Assessment:** VENDOR shall conduct an annual security assessment that identifies, categorizes and quantifies the security risks to data accessed, processed, transmitted and/or stored on behalf of HCSC. Identified gaps shall be addressed through documented remediation plans that shall be made timely available to HCSC upon request.
3. **Security Officer:** VENDOR shall appoint an individual who is either formally designated as a Security Officer and/or is responsible for compliance with and enforcement of the provisions of the Health Insurance Portability & Accountability Act (HIPAA) and other applicable current State or Federal regulation(s).
4. **Policies & Procedures:** VENDOR shall implement security policies and procedures to prevent, detect, contain and correct security violations, as well as to document the administrative, technical and physical controls in place to protect HCSC data. Upon request from HCSC, VENDOR shall provide a summary of security policies and procedures. Policies shall include appropriate disciplinary or sanction provisions to address data security violations. If VENDOR is accessing the HCSC network, VENDOR must comply with HCSC security policies and procedures.
5. **Awareness & Training:** VENDOR shall implement a data security awareness and training program for all members of its workforce, including management. Personnel assigned to access, process, transmit and/or store HCSC Protected Health Information (“PHI”) or Sensitive Personal Information (“SPI”) data, or Business Confidential Information (“BCI”) shall receive formal training prior to contact with HCSC data. BCI means any business or technical information in any form or medium related to HCSC’s business. In those instances where VENDOR personnel shall access PHI/SPI via the HCSC network from a remote location, VENDOR personnel shall also be required to complete specific HCSC regulatory training prior to contact with such data.
6. **Security Monitoring:** VENDOR shall continuously monitor security events and conduct periodic reviews of its information system activities. Events deemed to be suspicious shall be investigated. VENDOR shall implement appropriate hardware, software and/or procedural audit control mechanisms that record and examine activity in information systems that access, transmit, process and/or store HCSC data.
7. **Incident Response:** VENDOR shall implement and maintain a security incident response program that includes:
	1. Timely notification to HCSC in the event HCSC data is known to be or suspected to have been compromised. The term “timely notification” shall be defined as providing notice to HCSC as soon as possible after the VENDOR becomes aware of a known or suspected security incident including a data breach—but in no event more than five (5) business days or if applicable, per the terms of their Business Associate Agreement, after VENDOR first became aware that a data breach may have occurred. For purposes of this section, a suspected security incident does not include pings and other broadcast attacks on VENDOR’S firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as such incidents do not result in, nor are suspected to have resulted in, unauthorized access, use or disclosure of HCSC data.
	2. Appropriate containment and mitigation steps to prevent further damage from any compromising incident, as well as corrective action steps to prevent a similar incident from recurring.
8. **Facility & Workstation Security:** For any VENDOR facility that houses personnel or systems used in the viewing, processing, or storing of HCSC data, VENDOR shall comply with the following security requirements:

| **Security Requirement** | **Data Center Within the U.S.** | **Office Located Within the U.S.** | **Office Located Outside of U.S.** |
| --- | --- | --- | --- |
| Monitor building exterior and all entrances. | X | X | X |
| All doors located on the outer perimeter shall be constructed to prevent unauthorized access, shall be alarmed or monitored and shall be designed to resist forced entry. | X | X | X |
| Deploy and monitor cameras 24x7, with feed to a central location and DVD-based recording with video backup which is preserved and maintained by the VENDOR for no less than 30 days. | X |  | X |
| Deploy and use an electronic access control system for perimeter and high-security areas, including the area where HCSC-related functions shall be performed. | X |  | X |
| Restrict access to VENDOR facilities in a secure, auditable manner. Each employee should have a unique key, access card, or key code assigned to them. | X | X | X |
| Have a process for logging and escorting visitors. Said process shall require visitors to: - sign in and out- produce photo identification- be escorted at all times- only be granted access for specific, authorized purposes | X | X | X |
| Have solid floor-to-ceiling walls (slab to slab construction) in the designated area where HCSC-related functions shall be performed. | X |  |  |
| Provide alternate power sources, such as generators, uninterruptible power supply (“UPS”) to the network equipment required to carry out HCSC functions. | X | X | X |
| Not display anything associated with the HCSC corporate name or logo or the location of the facility to which they permit access on Personnel ID badges or locations outside of the HCSC production area. | X | X | X |
| All HCSC data received or created in paper form, or stored / contained within other portable media, must be stored in locked containers, locked offices, or other controlled secured areas when not needed for servicing the HCSC account. However, this rule is not applicable to any VENDOR facility dedicated solely to HCSC or HCSC services. | X | X | X |
| Laptops and mobile devices shall not be used to access, process, transmit, or store HCSC data unless data stored within, or transmitted to or from the laptops or mobile devices are encrypted as per Section 9. | X | X | X |
| Mobile devices and laptop computers are prohibited in any HCSC production area, except as authorized by HCSC. |  |  | X |
| Individuals desiring entry into the HCSC production area are subject to search by security personnel prior to admittance. |  |  | X |
| Handbags, briefcases, backpacks and other similar items are prohibited in any HCSC production area. |  |  | X |
| Restricted access parking shall be in place and require vehicle identifiers, examination prior to entrance (visual inspection of undercarriage, interior of vehicle, interior of trunk, etc.), and presentation of employee identification badge required prior to entrance. |  |  | X |
| Workstations shall be positioned so that HCSC data is not visible to unauthorized personnel. | X | X | X |
| Workstations shall lock after no more than 10 minutes of inactivity. However, VENDOR personnel shall be instructed to lock their workstations when they shall be away from their desks. | X | X | X |
| Print capability shall be limited to printers located within VENDOR’s facilities within the U.S. and disabled for all other locations. | X | X | X |
| Access to applications shall be limited. Applications not required for processing HCSC data shall be disabled. | X | X | X |
| Portable storage device drives shall be disabled (i.e. USB, CD/DVD). | X | X | X |
| End-point firewalls shall be installed on all VENDOR workstations used for HCSC functions and shall be configured to prevent unauthorized network access attempts. | X | X | X |
| Operating systems and application software used must be currently supported by the manufacturer. | X | X | X |
| VENDOR shall maintain and enforce a Clean Desk policy. A Clean Desk policy shall include, but not be limited to the following: workers shutting down or logging off of their desktop computers during non-working hours and storing all paper or portable media containing HCSC PHI, SPI, or BCI in a locked drawer or cabinet, or secured in a locked office during non-working hours. | X | X | X |

1. **Encryption:** Where encryption is necessary or required to secure PHI or SPI, VENDOR must use encryption methods and technologies for data at rest and data in transit that comply with standards provided by the National Institute of Standards and Technology (NIST). VENDOR must use encryption technologies that comply with NIST Federal Information Processing 140-2 *Security Requirements for Cryptographic Modules* and applicable state and federal regulations (“Approved Encryption”).
2. **Physical Movement of HCSC Data**: With the exception of backup tapes that are securely transported to an off-site storage facility, HCSC data must not be removed from or physically transferred to non-VENDOR facilities without the written approval of HCSC.
3. **Data Disposal and Destruction:** Except where required to return data to HCSC upon termination or expiration of agreement, VENDOR must securely dispose of or destroy HCSC PHI, SPI, BCI, and work product information, when such information is no longer necessary for Services rendered under this agreement, or at any time upon request from HCSC. Data shall be disposed of and destroyed in a secure manner to ensure that no inadvertent disclosure of the data is possible. In the event that secure disposal or destruction is not possible, VENDOR shall continue to secure the data at a level equivalent to this contract and as required by law.
4. **Remote Access:** Remote access to systems or networks that contain HCSC data must use multi-factor authentication and an encrypted connection as per Section 9.
5. **Asset Tracking:** VENDOR shall ensure that all assets:
6. Owned by VENDOR and used in the performance of HCSC-related functions shall be returned by VENDOR personnel upon personnel’s termination from VENDOR.
7. Owned by HCSC shall be returned to HCSC upon HCSC’s request or upon termination of contract with HCSC.
8. Containing HCSC data that are end-of-life shall be securely destroyed.
9. Unless approved in writing by HCSC, VENDOR shall not store any HCSC PHI/SPI data on portable media. If authorized by HCSC to store HCSC data on portable media, the portable media shall be encrypted as per Section 9. When data on the portable media is no longer required, VENDOR shall have a secure disposal/destruction policy that shall be followed to ensure that the data on the media cannot be retrieved.
10. **Anti-Malware:** VENDOR shall ensure the servers and workstations involved with accessing, processing, transmitting or storing HCSC data are protected with up-to-date anti-malware software. VENDOR shall have a process in place for issuing regular updates to anti-malware software and conducting regular scans of the environments containing HCSC data.
11. **Logical Separation of HCSC Data:** HCSC data shall be logically separated from data of other VENDOR accounts.
	* + - 1. **Non-Production Environments**: HCSC PHI and SPI must be de-identified before it can be migrated to a non-production environment (*e.g.* testing or development). If de-identification is not possible, then the data must not be migrated into any non-production environment unless the non-production environment offers the same level of security controls used to safeguard the data in the production environment.
12. **Access to Data:** VENDOR shall ensure that only its employees with a need to know (*aka* “minimum necessary” or “rule of least privilege”) have appropriate access to HCSC data. In addition to any other safeguards necessary to comply with this requirement, VENDOR also agrees to maintain the following controls;
13. Access to HCSC data and systems that contain HCSC data must be access controlled through the use of appropriate authentication controls.
14. Termination of access to VENDOR systems used to access, process, transmit or store HCSC data shall be as immediate as possible.
15. In instances where a VENDOR employee has access to the HCSC network, VENDOR shall notify HCSC within 24 hours if an individual no longer works for VENDOR or no longer works on the HCSC account.
16. Audit trail records must be generated and retained whenever HCSC PHI or SPI has been altered, moved, copied, or deleted. The audit trails must identify the user(s) or system(s) that altered, moved, copied, or deleted the data.
17. Conducting periodic reviews of access to HCSC systems and/or data, at least annually.
18. Issuing a unique user identifier and password to each individual who shall be using, processing, or storing HCSC data. At a minimum, user account passwords shall:
19. Be protected at all times during their life-cycle.
20. Be at least 8 characters in length
21. Expire and require a password reset at least once every 60 days
22. Not be a previously used password for at least 6 password generations
23. Contain a mixture of alpha (A, B, C), numeric (1, 2, 3), and special characters (#, %, &)
24. Suspend the account after 3 consecutive failed login attempts
25. Be stored in an encrypted format
26. Require initial user passwords be changed on first use
27. Require default vendor passwords be changed.
28. **Patch Management:** VENDOR shall have a patch management policy and process in place that provides for the application of all current patches in a timely manner for all systems and applications that receive, maintain, process or otherwise access HCSC data.
29. **Network Security:**
30. VENDOR shall implement and maintain intrusion detection to monitor the network and detect any anomalies that would be addressed through a formal incident response process.
31. VENDOR shall partition its infrastructure into security zones with flow control devices, such as firewalls and routers, which govern the allowable flows between security zones, which enable VENDOR to deploy a defense-in-depth architecture.
32. Networks that contain HCSC data must be separated from public networks by a firewall to prevent unauthorized access from the public network.  HCSC data must not be stored on Internet accessible networks or network segments.
33. **Development & Testing:** If VENDOR personnel are involved with application development and/or testing on the HCSC network, they shall follow HCSC’s change management procedures. If the work is performed on VENDOR systems, VENDOR shall have appropriate change management procedures to prevent unauthorized activities from occurring in test, development or production.
34. **Business Continuity/Disaster Recovery:** In addition to the requirement that VENDOR maintain Business Continuity/Disaster Recovery (“BC/DR”) plans and programs, as part of those BC/DR programs VENDOR shall also:
35. Test those BC/DR plans and programs on a regular and periodic basis. Upon request from HCSC, VENDOR shall provide a summary of the results of those tests and any associated remediation plans.
36. Establish and maintain a crisis management process, designed to enable VENDOR to address crises as they arise. The process requires all sites/locations with personnel to create an Emergency Plan. The Crisis Management process is activated immediately when an actual or potential crisis situation arises.
37. Maintain backups, to occur regularly, for VENDOR systems used to access, process, transmit or store HCSC PHI/SPI data. VENDOR shall have a formal backup/recovery strategy. Backups must be encrypted and stored in an environmentally protected, physically secure off-site facility.
38. Notify HCSC within four (4) hours of a declared disaster advising of the situation and any impact to HCSC functions and PHI/SPI data.

In the event that the terms and conditions contained in this Addendum are different than, or conflict with, the terms and conditions contained in the underlying agreement, the terms and conditions contained in this Addendum shall govern, with the exception of the Business Associate Agreement, if applicable.

**Health Care Service Corporation,**

**a Mutual Legal Reserve Company**

**“HCSC” “VENDOR”**

|  |  |
| --- | --- |
|  |  |
| By: |  | By: |  |
|  |
| Name: |  | Name: |  |
|  |
| Title: |  | Title: |  |
|  |
| Date: |  | Date: |  |