SECURITY REQUIREMENTS

Company represents and warrants that it has implemented a written information security program ("Information Security Program") that includes administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and availability of DaVita's Confidential Information, and meets or exceeds the Security Requirements set forth below. Any capitalized term not defined in these Security Requirements has the meaning assigned to it in the Agreement giving rise to the engagement between Company and DaVita.

1. Unique User IDs and Passwords. Company will not create any generic accounts and Personnel accessing DaVita systems will:
    a. Be assigned a unique identifier (i.e., user name);
    b. Have only one identifier (e.g., user has only one account); and
    c. Not share user IDs or passwords.

2. Company Personnel System Access Control Policy and Requirements.
    a. Company will control Personnel's access to DaVita Confidential Information and DaVita IT resources using the principle of least privilege.
    b. At a minimum, Company must selectively restrict access to DaVita Confidential Information and IT resources based on the duties assigned to each Personnel.
    c. Upon DaVita's request, Company will supply DaVita with a current list of Personnel having access to DaVita Confidential Information or IT resources, including the job duties and permissions associated with each individual.
    d. DaVita may, at any time, require Company to make changes to the access list, including denying any Personnel access to DaVita Confidential Information and IT resources.

3. Company Network Security Control Requirements.
    a. All remote access to DaVita Confidential Information and IT resources by Authorized Personnel will use the DaVita virtual private network ("VPN").
    b. Any transmission of DaVita Confidential Information must be encrypted with a strong commercial algorithm that uses at least a 256AES-bit encryption key or equivalent.
    c. Any transfers of DaVita Confidential Information to a third party must be approved by DaVita in writing in advance.

4. Company Site Physical Controls. Systems containing DaVita Confidential Information must be secured, using the following, to restrict access to appropriately authorized Personnel:
    a. Located behind steel locked doors, protected by cardkeys, combination locks, or biometric devices; and
    b. Key access with alarm systems and/or video surveillance systems, when not manned.

    Company must implement environmental controls including but not limited to temperature, humidity, static electricity and fire suppression.

5. Company Firewall, Intrusion Detection and Intrusion Prevention. Company must (i) employ an appropriate firewall and IPS/IDS that meet or exceed industry standards and (ii) ensure that all access to DaVita IT resources and/or Confidential Information, and all traffic to and from the Company's and DaVita's sites occurs exclusively through such firewall and IPS/IDS.

6. Patching and Malware Protection on Company IT Systems. Company must:
    a. Keep its software (operating systems, databases, applications, device drivers, etc.) current and install applicable service packs, fixes, and patches for software no less frequently than weekly.
    b. Install commercial anti-virus and malware protection on all Company systems (including IT servers, workstations, laptops, etc.) used to store, process or transmit DaVita Confidential Information.
    c. Update all anti-virus and malware protection at least daily.

7. Encryption and Data Loss Prevention. All Company systems that access DaVita Confidential Information must use commercial data loss prevention media encryption that provides:
    a. Full disk encryption for internal and external drives; and
    b. Encryption of all removable media, including but not limited to, DVDs, CDs, flash drives, and plug-in drives.

8. Security Awareness and Training. Company will require all Personnel and their management to successfully complete a security awareness and training program, no less than annually, which includes training on how to implement and comply with its Information Security Program.

9. Assigned Security Responsibility. Company will designate a security official responsible for the development, implementation, and maintenance of its Information Security Program, and inform DaVita of the identity of such official.

10. Termination of Personnel. Upon the voluntary or involuntary separation of any Personnel, Company will promptly:
    a. Delete all system access credentials for such Personnel;
    b. Notify DaVita in writing so that DaVita can remove such person's access to DaVita systems and/or facilities;
    c. Recover any keys, cards or other items used to access physical facilities; and
    d. If applicable, change Company access codes and alarm codes.

11. Security Incident Procedures - Company will employ automated controls to detect, respond to, and otherwise address security incidents, including but not limited to unauthorized access, acquisition, disclosure or use of PII ("Security Incident"). The controls will include procedures to monitor systems and to detect actual and attempted attacks on or intrusions into PII or information systems relating thereto, and procedures to identify and respond to suspected or known Security Incidents, mitigate harmful effects of Security Incidents, and document Security Incidents and their outcomes.

12. Security Breach Reporting - Within 72 hours of discovering any Security Incident or security breach involving DaVita's Confidential Information and/or IT systems, Company will:
    a. Identify the nature of the non-permitted use or disclosure including how the use or disclosure was made;
    b. Identify the DaVita Confidential Information that was used or disclosed;
    c. Identify the person or entity who improperly received the non-permitted disclosure;
    d. Identify what corrective action Company took or will take to prevent further non-permitted uses or disclosures;
    e. Identify what Company did or will do to mitigate any deleterious effect of the non-permitted use or disclosure; and
    f. Provide DaVita with a written report that includes items "a" through "e" in this section 12.

13. Destruction or Removal of all DaVita Confidential Information from Company Storage – Company will purge its computer storage devices, including but not limited to, hard drives, CD's, floppies, and tapes, of all DaVita Confidential Information:

    a. At the end of the Agreement;
    b. Upon DaVita's request at any time; and
    c. Prior to discarding or reusing such device.

    Company may use any of the following methods for destroying or removing DaVita Confidential Information:

    a. DoD level reformatting with at least 3 passes overwriting data;
    b. Professional degaussing; or
    c. Physically destroying the storage media.

    Company shall keep records of the destruction, degaussing or secure reformatting of media, and provide such written records to DaVita upon request.

14. Subcontractors - Company will not use subcontractors without DaVita's prior written agreement. Company's use of permitted subcontractors will meet or exceed the following requirements:
    a. Company will employ policies and procedures to ensure that Company's use of permitted subcontractors does not compromise the security of DaVita's Confidential Information or IT systems.
    b. Company's policies and procedures, and Company's agreements with its subcontractors, must allow for immediate termination of a subcontractor or subcontractor employee upon discovery of a significant security breach.
    c. Company will prohibit subcontractors, and their employees, from accessing any DaVita data or system where such access is not required for Company to perform under this agreement.
    d. Company will audit its permitted subcontractors no less than annually to review its subcontractors' compliance with these Security Requirements and will provide DaVita with the results of the audit promptly upon completion of the audit.
    e. In the event that a permitted subcontractor fails an audit, Company will, as appropriate or as requested by DaVita, require subcontractor to take corrective action (including potentially terminating the subcontractor employees responsible for the failure(s)) or terminate subcontractor.

15. Attestations. Company will assist DaVita, in any way requested, to prepare any offshore or other Company attestations required by the Centers for Medicare and Medicaid Services or any other state or federal agency.

16. Notification of Non-Compliance. Company will notify DaVita of any noncompliance with these Security Requirements immediately upon discovery and identify any compensating controls in place. DaVita will perform a risk analysis assessing the exposure to DaVita resulting from the noncompliance. Company will, as requested by DaVita (a) remediate the non-compliance, or (b) provide compensating controls that (i) are as strong as or stronger than the non-compliant items and (ii) reduce risks to levels that DaVita deems acceptable in its sole discretion.

17. Right to Audit, Monitor or Verify. DaVita reserves the right to audit, monitor and verify Company's compliance with these Security Requirements and to use a third party to conduct such audit, monitoring and/or verification.