VENDOR HEALTH INFORMATION POLICY

PURPOSE: To provide guidelines to DaVita with respect to Vendors' access, use, disclosure, and protection of DaVita Protected Health Information (PHI) in accordance with HIPAA, specifically 45 CFR §§ 164.502(e) and 164.504(e), and in accordance with the VA Privacy Requirements.

DEFINITION(S):

Amendment Request: An Amendment Request is a request made by a patient or a patient's Personal Representative to DaVita's Business Associate to change certain information contained in the patient's medical record.

Breach: The acquisition, access, use, or disclosure of PHI in a manner not permitted by HIPAA or applicable state law, which compromises the security or privacy of the PHI.

Business Associate:

a. A Business Associate is a Vendor who has entered into a BAA with a Covered Entity (such as DaVita), and:

    i. On behalf of the Covered Entity, creates, receives, maintains or transmits PHI for a function or activity regulated by HIPAA, including but not limited to claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and repricing; or

    ii. Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services to or for the Covered Entity, where the provision of the service involves the disclosure of PHI from the Covered Entity, or from another Business Associate of the Covered Entity, to the Vendor.

b. Business Associate includes:

    i. A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to PHI to a Covered Entity and that requires access on a routine basis to such PHI;

    ii. A person that offers a personal health record to one or more individuals on behalf of a Covered Entity; and

    iii. A Subcontractor that creates, receives, maintains, or transmits PHI on behalf of a Covered Entity's Business Associate.

c. Business Associate does not include a health care provider, with respect to disclosures by a Covered Entity health care provider to another health care provider regarding the Treatment of a patient.

Business Associate Agreement (BAA): Agreement between a Vendor and DaVita, governing the Vendor's use or access of DaVita PHI accessed in the process of delivering the goods and/or services covered by the Services Agreement.

Covered Entity: A health care provider (e.g., doctor, dialysis facility, hospital, pharmacy, nursing home) that transmits health information electronically, a health plan (e.g., HMO, medical plan), or a health care clearinghouse (e.g., billing services).

Data Use Agreement: A Data Use Agreement is a written agreement that:

a. Establishes the permitted uses and disclosures of a Limited Data Set by the recipient (which must be solely for research, public health, or Health Care Operations purposes). The Data Use Agreement may not authorize the recipient of the data to further use or disclose the information in the Limited Data Set in a way that would violate HIPAA if done by DaVita;

b. Establishes who is permitted to use or receive the Limited Data Set; and

c. Provides that the Limited Data Set recipient will (i) not use or further disclose the information other than as permitted by the Data Use Agreement or otherwise required by law; (ii) use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the Data Use Agreement; (iii) report to DaVita any use or disclosure of the information not provided for by the Data Use Agreement of which it becomes aware; (iv) ensure any agents to whom it provides the Limited Data Set agree to the same restrictions and conditions that apply to the Limited Data Set recipient with respect to such information; and (v) not identify the information or contact the individuals.

DaVita: DaVita HealthCare Partners Inc., and its affiliates and subsidiaries.

De-identified: Data that is considered anonymous under HIPAA when:

a. The following identifiers of the patient and of the patient's relatives, employers and household members, are completely removed and DaVita has no knowledge that the information could be used alone or in combination with other information to identify a patient:

   i. Names;

   ii. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code where the

Bureau of Census data indicates that the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people, and the initial three digits for all such geographic units containing 20,000 or fewer people is changed to 000;

iii. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that ages and elements may be aggregated into a single category of 90 or older;

iv. Telephone numbers;

v. Fax numbers;

vi. Electronic mail addresses;

vii. Social security numbers;

viii. Medical record numbers;

ix. Health plan beneficiary numbers;

x. Account numbers;

xi. Certificate/license numbers;

xii. Vehicle identifiers and serial numbers, including license plate numbers;

xiii. Device identifiers and serial numbers;

xiv. Web Universal Resource Locators (URLs);

xv. Internet Protocol (IP) address numbers;

xvi. Biometric identifiers, including finger and voice prints;

xvii. Full face photographic images and any comparable images; and

xviii. Any other unique identifying number, characteristic, or code, except for certain permitted record identification codes used for re-identifying the information; ***OR***

b. A qualified Statistician determines, and documents the methods and analysis leading to such determination, that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient, to identify a patient who is the subject of the information.

Electronic Protected Health Information (ePHI): Electronic Protected Health Information is any Protected Health Information which is transmitted or maintained by or in electronic media.

Financial Remuneration: Direct or indirect payment from or on behalf of a Third Party whose product or service is being described. Direct or indirect payment does not include any payment for Treatment of a patient.

Health Care Operations: Certain administrative, financial, legal, and quality improvement activities necessary to run a health care business and to support the core functions of Treatment and Payment. A summary of these activities, as defined at 45 CFR § 164.501, include:

a. Conducting quality assessment and improvement activities, patient safety activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination;

b. Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities;

c. Except as prohibited with respect to certain genetic information, underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims;

d. Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs;

e. Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and

f. Business management and general administrative activities, including those related to implementing and complying with the Privacy Rule and other Administrative Simplification Rules, customer service, resolution of internal grievances, sale or transfer of assets, and creating De-identified health information or a Limited Data Set.

HIPAA (to be inclusive of HITECH): Health Insurance Portability and Accountability Act of 1996, the "Privacy Rule" (45 CFR Parts 160 and 164, subparts A and E), the "Security Rule" (45 CFR Part 164, subparts A and C), and the federal "Breach Notification Rule" (45 CFR Part 164, subpart D), as amended or added by the Health Information Technology for Economic and Clinical Health Act ("HITECH") and its implementing regulations (collectively "HIPAA").

IT Resources: All hardware and software including, but not limited to, host computers, files, applications, communications, email, fax, intranet, print servers, Workstations, stand-alone computers, laptops, handhelds, mobile phones, printers, software, hubs, switches, routers, cables, and all other internal and external computer and communications resources and devices which may receive, transmit, and/or store DaVita PHI.

Limited Data Set: A Limited Data Set is PHI that excludes the following direct identifiers of the patient or of relatives, employers or household members of the patient:

a. Names;
b. Postal address information, other than town or city, State, and zip code;
c. Telephone numbers;
d. Fax numbers;
e. Electronic mail addresses;
f. Social security numbers;
g. Medical record numbers;
h. Health plan beneficiary numbers;
i. Account numbers;
j. Certificate/license numbers;
k. Vehicle identifiers and serial numbers, including license plate numbers;
l. Device identifiers and serial numbers;
m. Web Universal Resource Locators (URLs);
n. Internet Protocol (IP) address numbers;
o. Biometric identifiers, including finger and voice prints; and
p. Full face photographic images and any comparable images.

Manager: Teammate who manages the overall operations at a DaVita location or within a DaVita department.

Marketing:

a. Marketing includes:
    i. A communication about a product or service that encourages recipients of the communication to purchase or use the product or service.
    ii. An arrangement between a DaVita business and any other person or company whereby the DaVita business discloses PHI to the other person or entity, in exchange for money or other form of reimbursement, so the person or company can contact patients or their Personal Representatives about its own product or service and encourage them to purchase the product or service.
b. Marketing does not include communications about products or services with patients or their Personal Representatives when:
    i. A communication is made to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the patient, but only if any Financial Remuneration received by DaVita in exchange for making the communication is reasonably related to the cost of making the communication.
    ii. A communication is made for the following Treatment and Health Care Operations purposes of the DaVita, ***except*** where DaVita receives Financial Remuneration in exchange for making the communication:

1. For Treatment of a patient by a health care provider, including for case management or care coordination for the patient, or to direct or recommend alternative treatments, therapies, health care providers or settings of care to the patient;
2. To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, DaVita, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or
3. For case management or care coordination, contacting of patients or their Personal Representatives with information about Treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

Minimum Necessary: The most minimal amount of PHI that would reasonably be needed to accomplish an intended use, disclosure or request.

Payment: Includes activities taken by a health care provider Covered Entity (e.g., DaVita, DaVita Rx) to obtain or provide reimbursement for the provision of health care, including (i) determinations of eligibility or coverage, (ii) risk adjustments; (iii) billing, claims management, collection activities, reinsurance activities, and related data processing; (iv) medical necessity or other review for justification of charges; (v) utilization review activities; and (vi) required disclosures of certain PHI to consumer reporting agencies relating to collection of premiums or reimbursement.

Personal Representative: An individual who is legally appointed, designated and/or authorized pursuant to state law to: (a) make health care decisions on behalf of a patient, or (b) act on behalf of a deceased individual or a deceased individual's estate. In the case of a VA Patient, the term "Personal Representative" shall mean a VA Patient Personal Representative.

Privacy Act: The Privacy Act of 1974, 5 U.S.C. § 552a and the implementing regulations of the VA set forth at 38 C.F.R. §§ 1.575-1.584.

Protected Health Information (PHI):

a. PHI is any individually identifiable information that is maintained or transmitted about a patient in any form, including electronic, that:
    i. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse;

ii. Relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and

iii. Identifies or could be used to identify an individual.

b. PHI excludes individually identifiable health information:

i. In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

ii. In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);

iii. In employment records held by a Covered Entity in its role as an employer; and

iv. Regarding a person who has been deceased for more than 50 years.

Secretary: The Secretary of Health and Human Services (HHS) or any other officer or employee of HHS to whom Secretarial authority has been delegated.

Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Services Agreement: Documented agreement and/or other arrangement pursuant to which a Vendor provides products and/or services to DaVita that may require Vendor to access, create and use health information including but not limited to PHI that is protected by state and/or federal law.

Statistician: A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable.

Subcontractor: means a person to whom a Business Associate delegates a function, activity, or service otherwise required to be performed by the Business Associate under its Services Agreement or BAA with a Covered Entity, other than in the capacity of a Teammate of such Business Associate.

System of Records: Any group of records under the control of a Federal agency or its contractors from which information may be retrieved by the name of the individual, or by some identifying number, symbol, or other personal identifier. The maintenance of a System of Records is published by a notice in the Federal Register. Single records or groups of records which are not retrieved by a personal identifier are not part of a System of Records. Papers maintained by individual employees of the Federal agency (or its contractors) which are prepared, maintained, or discarded at the discretion of the employee and which are not subject the Federal Records Act (44 U.S.C. 2901) are not part of a System of Records, provided that such personal papers are not permitted to be accessed or reviewed by persons not sworn to confidentiality.

Teammate: Employees and other persons whose conduct, in the performance of work for DaVita, is under the direct control of DaVita, whether or not they are paid by DaVita. The term "Teammates" excludes volunteers, trainees, student interns and Medical Directors.

Third Party: A Third Party is someone other than:

a. The patient or the patient's Personal Representative;

b. DaVita; or

c. A Teammate of DaVita.

Treatment: Includes direct treatment of the patient or the coordination or management of the patient's health care with other providers, including referrals of patients from one health care provider to another (*i.e.*, primary care provider, ERs, acute dialysis teams, nursing homes, home health agencies, etc.).

Unauthorized Use or Disclosure: Any acquisition, access, use, or disclosure of PHI that is not permitted by HIPAA, the VA Privacy Requirements, applicable state law, or DaVita HIPAA Privacy Policies and Procedures.

Unsecured PHI: PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through destruction of the PHI or encryption of the PHI, or such other technologies or methodologies specified by the Secretary from time to time.

VA: United States Department of Veterans Affairs.

VA Confidentiality of Certain Medical Records Statute: The VA statute regarding the confidentiality of records relating to treatment of VA Patients' drug abuse, alcoholism or alcohol abuse, infection with the human immunodeficiency virus, or sickle cell anemia, 38 U.S.C. § 7332, and its implementing regulations set forth at 38 C.F.R. §§ 1.460-1.496.

VA Confidentiality of Medical Quality-Assurance Records Statute: The VA statute regarding the confidentiality of medical quality-assurance regulations, 38 U.S.C. § 5705, and its implementing regulations set forth at 38 CFR §§ 17.500-17.511.

VA Contractor: Any entity that is party to a written agreement with the VA, whereby such entity agrees to provide services to VA Patients.

VA Patient: A veteran or any other individual for whom the VA pays for medical care.

VA Patient Personal Representative: The parent of any minor, or the legal guardian of any individual who has been declared incompetent due to physical or mental incapacity or age by a court of competent jurisdiction. 38 CFR § 1.576(d).

VA Privacy Requirements: The privacy requirements applicable to VA Records set forth in the Privacy Act, the VA Confidentiality of Medical Quality-Assurance Records

Statute, the VA Confidentiality of Certain Medical Records Statute, and the VHA Handbook.

VA Records: Collectively, any record protected by the VA Privacy Requirements.

Vendor: Persons or organizations that provide, or seek to provide, goods or services directly to DaVita patients, DaVita Workforce members, or DaVita or one of its affiliated entities.

VHA: Veterans Health Administration of the VA.

VHA Handbook: The Department of Veterans Affairs, Veterans Health Administration Handbook 1605.1, privacy and Release of Information (May 1, 2006).

Workforce: DaVita teammates, volunteers, trainees, and other persons who conduct work on behalf of DaVita, and in the performance of work on behalf of DaVita are under the direct control of DaVita, whether or not they are paid by DaVita. Business Associates who have signed BAAs are not members of the Workforce.

Workstation: An electronic computing device (*e.g.* a laptop, desktop computer, or any other device that performs similar functions) and ePHI stored in its immediate environment.

POLICY:

1. Teammates must follow all applicable DaVita policies prior to disclosure of DaVita PHI to any Vendor, including obtaining appropriate approvals.

2. Vendors who are Business Associates are subject to, and must comply with, the applicable requirements of HIPAA, specifically 45 C.F.R. 164.502(e), the VA Privacy Requirements, and the underlying Services Agreement.

3. Notwithstanding anything in this Policy and Procedure to the contrary, each Vendor who is a Business Associate and who operates a VA System of Records on behalf of DaVita is required to have policies and procedures in place to comply with the provisions of the VA Privacy Requirements, as if such Vendor were a VA Contractor (i.e., an employee of the VA).

4. Vendors must sign a BAA before DaVita will allow access, use and/or disclosure of DaVita PHI, even if the disclosure is:
    a. Of only a Limited Data Set to a Vendor for the Vendor to carry out a Health Care Operations function, and DaVita has a Data Use Agreement with the Vendor;
    b. For DaVita's own Treatment, Payment, or Health Care Operations;
    c. For Treatment activities of another health care provider;

d. For Payment activities of another non-DaVita Covered Entity or health care provider; or

e. For Health Care Operations activities of another non-DaVita Covered Entity, if DaVita and such Covered Entity both have or had a relationship with the patient who is the subject of the PHI being requested (i.e., the patient is a common patient), the PHI pertains to such relationship, and the disclosure is:

   1. For the purpose of conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients (or their Personal Representatives) with information about treatment alternatives; and related functions that do not include Treatment;

   2. For the purpose of reviewing the competence or qualifications of health care professionals; evaluating practitioner and provider performance or health plan performance; conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers; training of non-health care professionals; accreditation, certification, licensing, or credentialing activities; or

   3. For the purpose of health care fraud and abuse detection or compliance.

5. Vendors must have appropriate policies and procedures regarding access, use, disclosure and safeguarding of DaVita PHI.

6. In the event DaVita knows of a pattern of activity or practice of a Business Associate that constitutes a material breach of the Business Associate Agreement, HIPAA, the VA Privacy Requirements, or DaVita's policies, DaVita will take any and all reasonable steps to remedy the breach or end the violation, up to and including termination of Service Agreements, if feasible.

7. Vendors will make available PHI so that the Covered Entity may satisfy its obligation to provide patients and their Personal Representatives the right to access the patients' PHI maintained in a Designated Medical Record Set. Provision of access will be addressed in accordance with the terms of their Services Agreement and BAA with the Covered Entity, any applicable policies and procedures of the Covered Entity, and HIPAA.

8. Vendors will make available PHI so that the Covered Entity may satisfy its obligation to provide patients and their Personal Representatives the right to amend the patients' PHI maintained in a Designated Medical Record Set. Provision of

Amendment Request will be addressed in accordance with the terms of their Services Agreement and BAA with the Covered Entity, any applicable policies and procedures of the Covered Entity, and HIPAA.

9. Vendors will make available PHI in their possession so that the Covered Entity may satisfy its obligation to provide patients and their Personal Representatives the right to an accounting of disclosures of the patients' PHI for up to six years (or such shorter time period at the request of the patient or Personal Representative) prior to the date the request for accounting was made. Provision of access will be addressed in accordance with the terms of their Services Agreement and BAA with the Covered Entity, any applicable policies and procedures of the Covered Entity, and HIPAA.

10. To the extent the Vendor is obligated under the Service Agreement to carry out one or more of DaVita's obligations under HIPAA or the VA Privacy Requirements, the Vendor will comply with the HIPAA requirements and VA Privacy Requirements that apply to the DaVita in the performance of such obligations.

11. Vendors must make their internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the Vendor on behalf of, DaVita available to the Secretary for purposes of determining DaVita's compliance with HIPAA.

12. At the termination of the Service Agreement, if feasible, Vendors must return or destroy all PHI received from, or created or received by the Vendor on behalf of, DaVita that the Vendor still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

13. To the extent any Subcontractor of a Vendor creates, receives, maintains, or transmits electronic PHI on behalf of the Vendor, such Vendor must ensure that such Subcontractor agrees to comply with the applicable requirements of HIPAA and the VA Privacy Requirements by entering into a written Business Associate Agreement with such Subcontractor that meets the requirements of both this Policy and Procedure and Vendor's underlying Services Agreement with DaVita.

PROCEDURES:

A. Permitted Use and Disclosures:

1. Vendors may access, use and/or disclose DaVita PHI, only if:
   a. Permitted by state and federal laws; and
   b. As limited by any:
      i. BAA;

ii. Services Agreement; or

iii. Valid HIPAA Authorization in conjunction with approval from DaVita.

2. DaVita may release DaVita PHI to a Vendor, if the patient (or Personal Representative) has signed a valid HIPAA Authorization in accordance with HIPAA.

3. Vendors will reasonably limit the amount of DaVita PHI that they access, use and/or disclose to the Minimum Necessary to accomplish the permitted purpose.

4. Vendors will ensure that the PHI they provide to their Subcontractors and agents is subject to the same restrictions that apply to the Vendor as described in this Policy and Procedure and under HIPAA and the VA Privacy Requirements, and will ensure that any Subcontractors that create, receive, maintain or transmit PHI on behalf of such Vendor agree to the same restrictions and conditions that apply to the Vendor with respect to such PHI.

5. A Vendor may use DaVita non-VA Patient PHI received by the Vendor in its capacity as a Business Associate of DaVita, if necessary, (a) for the proper management and administration of the Vendor; or (b) to carry out the legal responsibilities of the Vendor, ONLY IF (i) the disclosure is required by law; or (ii) the Vendor obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to such person, and the person notifies the Vendor of any instances of which it is aware in which the confidentiality of the information has been breached.

B. Non-Permitted Use and Disclosure:

1. Vendors will not be allowed to access, use and/or disclose DaVita PHI other than as permitted or required by the Business Associate Agreement, an underlying Services Agreement, a valid HIPAA Authorization in conjunction with approval from DaVita, and/or state or federal law.

2. Vendors will not sell, transfer, sub-license or disclose DaVita's PHI to any Third Party.

3. Vendors will not use or disclose DaVita's PHI for any Marketing activities.

4. Vendors will not use DaVita PHI to create De-identified information or Limited Data Sets, without written authorization from DaVita.

C. Safeguards: Vendors will use appropriate safeguards and comply, where applicable, with HIPAA's requirements regarding electronic PHI to prevent use or disclosure of the PHI other than as provided for by their Service Agreements.

1. Administrative: Vendors will:
    a. Have appropriate policies and procedures to protect the privacy and security of any DaVita PHI accessible to the respective Vendor and/or under the respective Vendor's control.
    b. Maintain the confidentiality of DaVita PHI and take steps to ensure Vendors' employees and agents do the same.
    c. Have procedures:
        i. For the authorization, supervision, and termination of access, use, and/or disclosure of DaVita PHI by their employees or agents.
        ii. To confirm their employees' or agents' access to DaVita PHI is appropriate and reasonable based on job functions and consistent with limitations of federal and state laws, and any applicable written agreements (e.g., BAAs, HIPAA Authorizations, etc.).
2. Physical: Vendors will:
    a. Not leave paper documents and records containing PHI in plain sight (or face up) when unattended or at the end of each workday.
    b. Dispose of DaVita PHI in a secure fashion (e.g., shredded, remove all data from hard drives, etc.) and as documented in the BAA.
    c. Not discard DaVita PHI or IT Resources containing PHI in trashcans without first rendering the DaVita PHI unreadable and unusable under HIPAA and in accordance with the BAA.
    d. Have appropriate locks on facility and office doors where DaVita PHI, both on paper and electronic media, may be stored.
    e. Retrieve all keys on or before an employee's last work day, and change locks as appropriate for employees who have access to DaVita PHI.
    f. Include confidentiality statements on emails and faxes containing DaVita PHI.
    g. Have password management policies and procedures, which prohibit:
        i. Sharing passwords that can access DaVita PHI;
        ii. Keeping written records of passwords; and
        iii. Use of "remember passwords" functionalities.
    h. Require employees and agents to physically protect IT Resources containing DaVita PHI.
3. Technical: Vendors will:
    a. Ensure that IT Resources under the respective Vendor's control that contain DaVita PHI are tracked, backed-up, and disposed of in a secure fashion and in accordance with the BAA.
    b. Require passwords to access IT Resources containing DaVita PHI.

c. Require employees and agents to log off, or use the "lock station" function, of computer terminals, from which DaVita PHI may be accessed prior to leaving the work area.

d. Password protect or encrypt DaVita PHI that is sent over the open internet.

e. Implement appropriate security controls on any IT Resource that may transmit or store DaVita PHI.

D. Security Breach Reporting:

1. Within 72 hours of discovery of any Breach of Unsecured PHI or Security Incident involving DaVita PHI, Vendors will report to DaVita the following information:

   a. Identify the nature of the non-permitted use or disclosure including how the use or disclosure was made;

   b. Identify the DaVita PHI that was used or disclosed;

   c. If possible, identify the person or entity who improperly received the non-permitted disclosure;

   d. Identify what corrective action the Vendor took or will take to prevent further non-permitted uses or disclosures;

   e. Identify what the Vendor did or will do to mitigate any deleterious effect of the non-permitted use or disclosure; and

   f. Provide DaVita with a written report.

Teammates are expected to report possible violations of this policy and procedure. You may make your report to an appropriate DaVita Manager, to the Corporate Compliance Hotline [(888)458-5848 or DaVitaComplianceHotline.com] or to DaVita's Corporate Compliance Department [(855)687-9645]. DaVita has a Non-Retaliation policy and will not tolerate any form of retaliation against anyone who files a Compliance report in good faith. Reports can be made anonymously or you may request confidentiality. Questions regarding this policy should be directed to the DaVita HIPAA Privacy Office by phone at (855)472-9822 or by email at HIPAA@DaVita.com.