Policy Title: Secure Electronic Storage of KP Non-Public Information	Policy Number: NATL.IS.004
Owner Department: Technology Risk Office	Effective Date: June 1, 2016
Custodian: Vice President, Technology Risk & Compliance	Page: 1 of 18

1.0 Policy Statement

Kaiser Permanente (KP) limits the storage of KP non-public information, including protected health information (PHI) and cardholder data (CHD), on computing systems/devices and removable/transportable electronic media.

2.0 Purpose

To describe requirements for protection of the confidentiality, integrity, and availability of KP non-public information stored electronically by KP.

3.0 Scope/Coverage

The provisions of this policy apply to the following persons (hereafter referred to "covered individuals"):

3.1 All employees of Kaiser Foundation Health Plan Inc. (KFHP), and Kaiser Foundation Hospitals (KFH) and their respective subsidiaries;

3.2 Members of the professional staffs of KFH hospitals;

3.3 All physicians and employees of the Permanente Medical Groups (PMGs);

3.4 All physicians and employees of The Permanente Federation LLC, and its subsidiary; and

3.5 All contractors, vendors, volunteers, students, or other persons providing paid or unpaid services to a KP entity or subsidiary.

3.6 Note: If any of the above individuals or KP organizations functions as a Business Associate to a non-KP entity, additional legal or contractual obligations and requirements may apply.

4.0 Definitions

See Appendix A – Glossary of Terms

5.0 Provisions

5.1 Storage of KP Non-Public Information (Excluding PHI)

5.1.1 Except when permitted by the provisions of this policy, KP Non-Public Information must be stored on data repositories that meet KP security standards.

5.1.2 Storage of credit card numbers (cardholder data) on any mobile or stationary endpoint device, or on removable/transportable electronic media, is prohibited. No exception is allowed.

5.1.3 KP encrypts all non-public information that is transferred from KP medical or computing systems/device to any type of removable/transportable electronic media (e.g., USB drives, removable hard drives, CDs and DVDs) except in cases where encryption is not possible.

5.2 Storage of PHI

5.2.1 Storage of PHI on any endpoint device or removable/transportable media by covered individuals is prohibited, except under conditions specified in provisions 5.2.2 and following.

5.2.2 Requirements for Approval of Storage of PHI. The decision maker for approval to store PHI on any laptop or mobile device, stationary device, or removable/transportable electronic media is a National Leadership Team member, Permanente Federation Executive Director, Regional President, or an Executive Medical Director (or his/her respective designee who must also be an executive in that organization and the sole person delegated for this purpose), who may approve an exception to the General Rule set forth in Provision 5.2.1 of this policy when the following conditions are met:

5.2.2.1 Storage of PHI on the specified device(s) is essential for the individual(s) to whom the approval applies to carry out his/her/their job; and

5.2.2.2 The specified device(s) and PHI will be encrypted consistent with standards specified in Provision 5.2 of this policy; and

5.2.2.3 The approval is for a specified duration and is in writing; and

5.2.2.4 The device is physically secured in accordance with the provisions of KP Information Security Policies *Premises Information Security and Privacy*, and *Mobile Computing and Teleworking*; and

5.2.2.5 The device (or electronic media, where technically possible) must have a strong password in the log-on procedure or for access in accordance with the KP IT standard on password management; and

5.2.2.6 When used to remotely access any KP network or medical or computing system/device, the device employs KP Technology Risk Office-approved two-factor authentication.

5.2.3 Automatic Exceptions. Archives of email messages containing PHI and residual data (that may or may not contain PHI) may be stored on an endpoint device or removable/transportable electronic media without approval otherwise required in Provision 5.2 of this policy under the following conditions:

5.2.3.1 The device or media has encryption technology that is installed, in use, and adheres to the current KP standard; and

5.2.3.2 The device or media is physically secured (e.g., locked room, locking cable for laptops and precautions while traveling, etc.) and protected by the covered individuals in accordance with the provisions of KP Information Security Policy, *Mobile Computing and Teleworking,* and/or, *Premises Information Security and Privacy*; and

5.2.3.3 The device requires a strong password in the log-on procedure or for access in accordance with the KP IT standard on password management; and

5.2.3.4 When used to remotely access any KP network or medical or computing system/device, the device employs KP Technology Risk Office-approved two-factor authentication.

5.2.4 Limited Exceptions Requiring Approval for Specified Research Studies: Collaborative research studies may involve collection and storage of PHI on non-KP-owned computing systems/ devices or electronic media. In the event that encryption of the computing system/device or electronic media is not a viable option for the study as structured, or will render the information unreliable or unusable, KP does not prohibit storage of non-encrypted PHI on such devices or media if:

5.2.4.1 The study has been approved by a KP Institutional Review Board (IRB) after being informed of the obstacle(s) to encryption; and

5.2.4.2 KP is satisfied that compensating controls have been implemented to prevent inappropriate unauthorized disclosure of the information; and

5.2.4.3 Subjects (members/patients) involved have signed an authorization and informed consent for study; and

5.2.4.4 Storage of the PHI on the computing system/device or removable/transportable electronic media has been approved in accordance with Provision 5.2 of this Policy.

5.3 Compliance Monitoring and Audit. Compliance officers monitor and conduct audits of the approval process and outcomes, and are responsible for notifying decision-makers of approvals that do not comply with this policy.

5.4 Corrective/Disciplinary Action

5.4.1 In accordance with applicable policies of KFHP, KFH or the relevant PMG, KFHP, KFH or the relevant PMG (each as relates to their respective employees, contractors and affiliates/partners) applies corrective/disciplinary actions against covered individuals found, after investigation by their respective employer or contracting party, to be in violation of this or another applicable policy, applicable law or KP's Principles of Responsibility. (See, e.g., National Human Resources Policy, NATL.HR.014, Corrective/Disciplinary Action, or the applicable Regional or Medical Group policy.)

5.5 Contractual Expectation of Third Parties

5.5.1 In the Vendor Code of Conduct, KP specifies requirements for vendors and contractors to comply with KP policies, legal and privacy requirements, such as HIPAA and KP National Privacy and Security Policy Business Associate Agreements - Requirements for Business Associates of KP Covered Entities NATL.NCO.PS.003 as well as setting forth KP expectations to avoid fraud, waste and abuse and furnishing of gifts to KP personnel. KP vendors and contractors can be subject to penalties or termination for failing to comply with the Vendor Code of Conduct.

5.5.2 Note: Third parties who are not vendors or contractors may be subject to different expectations (e.g., external researchers may be subject to actions by a KP Institutional Review Board or in accordance with Kaiser Foundation Research Institute policies).

6.0 References/Appendices

6.1 References:

6.1.1 Appendix A – Glossary of Terms

6.1.2 Information Security Policy, *Premises Information Security and Privacy*, NATL.IS.005

6.1.3 Information Security Policy, *Mobile Computing and Teleworking,* NATL.IS.013

6.2 Related Documents:

6.2.1 Health Insurance Portability and Accountability Act of 1996 (HIPAA):

6.2.1.1 U.S. Department of Health and Human Services. 45 Code of Federal Regulations Parts 160, 162, and 164; Health Insurance Reform: Security Standards, Final Rule (February 20, 2003)

6.2.1.2 U.S. Department of Health and Human Services. 45 Code of Federal Regulations Parts 160, 162, and 164; Health Insurance Reform: Privacy Rule, Final Rule (August 14, 2004).

6.2.2 Payment Card Industry Data Security Standard (PCI-DSS) 2.0. PCI Security Standards Council. Www.pcisecuritystandards.org. Wakefield, MA. 2010.

6.2.3 Sarbanes-Oxley Act of 2002 (Pub. L. No. 107-204, 116 Stat. 745), July 30, 2002.

6.2.4 National Institute of Standards and Technology (NIST) Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook.

6.2.5 National Institute of Standards and Technology (NIST) Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems.

6.2.6 International Standards Organization/International Electrotechnical Commission (ISO/IEC) Standard 17799, Information Security – Security Techniques – Code of Practice for Information Security Management.

6.2.7 Kaiser Permanente Clinical Technology, http://kpnet.kp.org/clintech/

6.2.8 Kaiser Permanente Information Technology General Controls 12.07.01, 12.10.01, 12.21.03, 12.21.08, 12.21.09, 12.21.12, 12.21.13, 12.22.01, 12.22.02, September 15, 2006.

7.0 Approval

The Secure Electronic Storage of KP Non-Public Information NATL.IS.004 policy is a result of restructuring the Information Security Policy NATL.IS.001 from a single policy into 17 separate policies. The requirements of this policy are not materially different from the requirements of the Information Security Policy NATL.IS.001, section 04.0.

The policy was reviewed and endorsed by the following representatives of Kaiser Foundation Hospitals, Kaiser Foundation Health Plan, Inc. and their subsidiaries, and the Permanente Medical Groups.

Name	Title	Organization	Date of Approval
Vanessa Benavides	Executive Vice President & Chief Compliance Officer	Kaiser Foundation Health Plan, Inc. & Kaiser Foundation Hospitals	12/16/2015
Richard Daniels	Executive Vice President & Chief Information Officer	Kaiser Foundation Health Plan, Inc. & Kaiser Foundation Hospitals	5/24/2016
Bill Wright, MD	President and Executive Medical Director	Colorado Permanente Medical Group, P.C.	8/19/2015
Geoffrey Sewell, MD	President and Executive Medical Director	Hawaii Permanente Medical Group, Inc.	6/17/2015
Bernadette Loftus, MD	Associate Executive Director	Mid-Atlantic States Medical Group, P.C.	7/30/2015
Jeffrey Weisz, MD	President and Executive Medical Director	Northwest Permanente, P.C.	4/30/2015
Edward Ellison, MD	Executive Medical Director and Chairman of the Board	Southern California Permanente Medical Group	6/1/2015
Patricia Conolly, MD	Associate Executive Medical Director	The Permanente Medical Group, Inc.	10/30/2015
Rob Schreiner, MD, FACP, FCCP	Executive Medical Director and Chairman of the Board	The Southeast Permanente Medical Group, Inc.	7/7/2015

Policy Revision History

Action[1]	Approval	Effective	Communicated
Original	10/01/2004	04/20/2005	04/20/2005
Revision	04/08/2009	05/30/2009	05/29/2009
Update	2/12/2010	02/12/2010	n/a
Revision	06/07/2012	02/01/2012	07/23/2012
Update	07/09/2014	07/08/2014	n/a
Updated	05/26/2016	06/01/2016	

[1] Update = No material change to the policy content, policy is reviewed and renewed with no, or non-material changes. Revision = Material change is included in the renewed policy.

Appendix A

Glossary of Terms

Activity – An action or occurrence detected and recorded by a computer program (e.g., successful and failed logging into or out of a computing system/device or non-exempt medical device; creating, reading, updating, or deleting any KP electronic information; modifying the configurations or settings of a computing system/device or medical device).

Affiliate – A third-party entity that provides services (typically medical) to KP members.

Auto-forwarding [email messages] – A rules-based or automated technology that intercepts incoming email and forwards it to another address. Auto-forwarding operates without action on the part of an individual.

Availability – The accurate and timely accessibility of data and resources to authorized individuals.

Backup – An exact copy of electronic information on a second medium (e.g., another server, compact disk, tape) kept as a precaution in case the original electronic information is damaged, destroyed, or becomes unavailable due to failure of the first medium or any other cause.

Biometric Indicator – A unique and measurable characteristic of a human being (such as a fingerprint, retina pattern, hand geometry, etc.) used to verify identity.

Business Application – Computer software that electronically performs a business process or task. Such applications may or may not be supported by KP-IT.A Business Application does not include operating system software, which integrates a computing device's capabilities and base functions. Business applications do not include end-user applications.

Business Application Owner – The individual responsible for ensuring an application consistently meets its stated business objectives and oversees application access and security and other legal requirements. The BAO is accountable for the application's development, use, maintenance, security, and functionality.

Business Continuity – The ability to continue primary and critical business functions, including patient care delivery, during and after an emergency or disaster.

Business Exposure – The extent to which a business is unprotected and open to damage, danger, or risk of suffering a loss.

Business Manager – A KP manager who is accountable for leading, managing, and administering activities and decisions related to KP information or KP IT infrastructure components (e.g., defining access criteria, approving accesses, and testing).

Business Supported Computing Systems/Devices – Computing systems/devices for which a KP business organization, rather than KP IT, formally provides support and maintenance. A KP business organization is a functional unit (e.g., Department of Pediatrics in a medical facility, Accounts/Payable in a Regional office) within KP that is not a part of KP IT.

Cardholder Data (CHD) – The full magnetic stripe of the Primary Account Number (credit or debit card number that identifies the issuer and the particular card holder), plus any of the following:

- Cardholder name
- Expiration date
- Service code.

Classification Authority – The party or entity that assigns a level of classification to a body of information.

Classified Information – Information officially mandated to be given special protection and that may be denoted with a special label in order to signify its status.

Clinical Technology – The functional units within KP that provide maintenance, asset management, and regulatory compliance services for diagnostic, therapeutic, and interventional medical equipment used in the delivery of patient care. Individual departments may be responsible for all or a subset (e.g., medical instrumentation, clinical laboratory equipment, medical imaging) of clinical technology equipment within a geographic region and may not necessarily have the phrase “clinical technology” in their names.

Computing Systems/Devices – Software and/or hardware used to store, transmit, and/or monitor electronic information, including information technology equipment that connects or potentially can connect to KP networks, whether owned by KP or not. Any printers, copiers, scanners, fax machines, or other equipment used for printing, copying, scanning, transmitting, or receiving non-public information, are connected to the KP network, and which may or may not be secured by physical or technical security controls, such as locked rooms, access keys, or user ID/account codes are considered computing systems/devices. Electronic storage media incapable of manipulating or processing data are not computing systems/devices.

Compensating Control – An internal control that reduces the risk of an existing or potential control weakness resulting in errors and omissions.

Confidentiality – The attribute of data or information being unavailable and not subject to disclosure to unauthorized persons or processes.

Contingency Planning – The KP policies and procedures established (for implementation as needed) to enable continuation of business operations in case of an emergency or disaster, including procedures to create and maintain exact copies of KP electronic information; restore lost data; enable continuation of critical business processes for protecting the security of KP electronic information and other components.

Control – A process or procedure implemented by management, the Board of Directors, or other key personnel, designed to provide reasonable assurance toward achievement of the company’s objectives through efficient and effective operations, reliable financial reporting, and compliance with applicable laws, regulations, policies, and other mandates.

Corrective/Disciplinary Action – Action by KP (including but not limited to retraining, reprimand, termination) to correct and/or sanction a covered individual for failure to comply with applicable laws, or KP’s *Principles of Responsibility.*

Covered Individuals – Those persons to whom the KP Information Security Policy applies, i.e.:

- All employees of Kaiser Foundation Health Plan Inc. (KFHP), and Kaiser Foundation Hospitals (KFH) and their respective subsidiaries;
- Members of the professional staffs of KFH hospitals;
- All physicians and employees of the Permanente Medical Groups (PMGs);
- All physicians and employees of The Permanente Federation LLC, and its subsidiary; and
- All contractors, vendors, volunteers, students, or other persons providing paid or unpaid services to a KP entity or subsidiary.
- Note: If any of the above individuals or KP organizations functions as a Business Associate to a non-KP entity, additional legal or contractual obligations and requirements may apply.

Critical Production Computing System – An application or other computing system supporting live, day-to-day operation of functions that are required for KP to continue its business.

Designated Record Set – A designated record set is any group of medical or health plan records that contains protected health information (PHI) and is used to make decisions about a member/patient (e.g., medical records; billing records; records of enrollment; payment and claims adjudication records; case or medical management records, each of which is a separate designated record set).

Designated Subset (of Structured Information) – A set of information that is either currently classified, or that will be gradually added over time to the body of classified information overseen by a classification authority.

Destruction – Rendering computing systems/devices, medical devices, or electronic media, or the information that they may contain unusable by breaking, burning, dismantling, or other physical means. Destruction of the device or media also destroys the information the device or media may have contained.

Disaster – A natural or man-made event causing significant damage or destruction that could or does interfere with the continuation of business operations. Examples include earthquakes, civil unrest, widespread storm damage, and acts of war.

Device Owner – A person owning a medical or computing system/device or removable/transportable electronic media that may, under certain conditions, be used for KP business.

Disaster Recovery – The ability to restore or resume operations and systems/devices following loss of computing systems/devices, medical devices, and/or data that may arise, for example, due to fire, system failure, or natural disaster.

Electronic Attack – A computer program that attempts or succeeds in disabling, taking over, or otherwise impairing access to or the performance of a computing system/device or medical device by exploiting a vulnerability (e.g., buffer overflow, denial of service).

Electronic Mail or Email – Messages, including text, graphics and attachments, electronically sent from one person to others (e.g., individual). Email includes messages sent over KP's local area network (LAN) or a dial-up service via an Internet Service Provider (ISP).

Electronic Media – Non-computing devices, e.g., diskettes, flash memory drives, CDs, DVDs, tapes, hard disks, internal memory, memory cards, and any other interchangeable, reusable, and/or portable electronic storage media (1) on which electronic information is stored, or (2) that are used to move data among computing systems/devices. Printers, copiers, faxes, scanners, and similar devices may contain information storage units; these storage units are considered electronic media and subject to all applicable controls.

Email System – Electronic communications technology system which creates receives or transmits email messages and may also include other functionalities including calendar and to-do lists.

Emergency – Localized situations that threaten the ability to continue information processing or other KP business and service functions. Examples include power failures and fire evacuations.

Encryption – The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a secret process or key.

End-User Application – Any software asset used to process, store, transmit, and/or monitor electronic KFHP/H financial data and transactions, where the end-user is responsible for defining and performing the data input (manually or through data-loading), manipulations (e.g., input, aggregation, selection, calculation, sort) and output processes. Examples of end-user applications include spreadsheets (e.g., MS Excel), database applications (e.g., MS Access, SAS, FOCUS), and word processing (e.g., MS Word).

Endpoint Computing System/Device – Any computing system/device that connects to or otherwise enables user interaction with computing systems and applications. Endpoint computing devices include desktop computers/workstations, laptop computers, and wireless handheld devices such as single- and multi-function mobile devices (e.g., PDAs and BlackBerrys), and telephonic devices (in particular, cell phones or other telephonic devices that are capable of receiving electronic data such as email).

Erase or Erasure – To make or cause to make information inaccessible, unreadable, unusable, or otherwise unrecoverable by using software or magnetic devices to overwrite or physically corrupt the information so that it cannot be restored to a usable state by commercial means.

Essential Electronic Information – Any electronic information, whose damage or destruction would impede patient care or the ability to meet legal, regulatory compliance, contractual, or business requirements, and accordingly must be backed up and otherwise protected from permanent loss.

Fax Back – Also called "fax on demand" is a recipient-controlled information delivery system in which the recipient's request for information from a computer (made via voice or telephone keypad input) results in the computer sending the requested information returned as a fax. Faxes sent by a fax machine are not considered Fax Back.

Group/Shared User ID/Account – A user ID/account assigned to a department or group instead of a single user. For example, in the in-patient hospital setting, a nursing station may share a group user ID to initially boot-up the computing system/device for the nursing station.

Health Care Provider – A medical professional (including physicians) who provides care.

Impact – The negative effect to KP that could result when a threat successfully exploits a vulnerability.

Information Classification – Grouping information according to its value to the organization based upon law, criticality to business functions, difficulty to reproduce, and possible consequences of loss, damage, or disclosure.

Information Security – Protection of information to insure confidentiality, integrity, and availability.

Information Security Policy Instrument – A standard or procedure that supports the implementation of an information security policy. Compliance with policy instruments must be measurable and auditable.

Integrity – The assurance that information or data is accurate and has not been altered or destroyed in an unauthorized manner.

IT-Related Content – Any document, text, or graphics, that communicates processes, procedures, settings, or specifications regarding the KP computing environment or computing systems/devices.

IT General Controls (ITGCs) – Those controls embedded in IT processes and services, such as systems acquisition or development, implementation, change management, security computer operations or disaster recovery. ITCG controls may also apply to server hardware used for application, database and utility processing, as well as hardware and software required for local and wide-area network connectivity.

KP – The Kaiser Foundation Health Plans, Kaiser Foundation Hospitals, Permanente Medical Groups, and their respective subsidiaries, except Kaiser Permanente Insurance Company (KPIC).

KP Information – Information in any form or media created by or on behalf of KP in the course and scope of its business, regardless of whether that information is maintained or stored by KP and others on KP's behalf. Examples of KP information includes, but is not limited to patient and member records, personnel records, financial information, company competitive information, KP-developed intellectual property, and business email messages.

KP Information Technology (KP IT) – The KP organization responsible for planning, designing, and overseeing implementation and ongoing operations of KP Information Technology (KP IT) computing systems/devices and networks.

KP IT-Supported Computing System/Device – Any computing system/device for which KP IT officially provides support and maintenance.

KP Premises – Any physical location owned or leased by KP in the conduct of KP business functions, including patient care delivery (for example, a building, or a KP floor, unit, or other interior or exterior area of a non-KP building).

KP-Owned Computing Systems/Devices – Any computing systems/devices purchased or leased with KP funds.

KP-Owned Electronic Media – Any electronic media purchased or leased with KP funds.

Law – A statute or other legislative enactment, regulation, constitutional provision, and case law.

Likelihood – The possibility that a given vulnerability would allow a negative event to occur given the motivation, capability, and nature of a threat. Likelihood is influenced by the existence and effectiveness of controls.

Malicious Program Detection/Remediation Software – Products designed to detect, disable, and/or remove a virus or other malicious programs introduced into a network or computing system/device.

Medical Device – Any device or system of devices directly involved in the acquisition, collection, interpretation, storage, transmission, and/or display of physiological data, delivery of life support assistance, or the delivery of therapeutic energy, for the purposes of providing patient care. Medical devices/systems may incorporate standard computing platforms (e.g., Windows or UNIX) and may be capable of transmitting or receiving data through proprietary or shared networks. Most medical devices/systems are certified through the U.S. Food and Drug Administration (FDA).

- **Exempt Medical Devices –** Devices which, because of their design or construction or because of the way the device is being used, cannot support or use security controls or settings required by KP even though the devices collect, store, transmit, or display electronic protected health information (PHI).
- **Security-enabled Medical Devices –** Devices that can support or use applicable security controls or settings required by KP.

Messaging Functions – Electronic means for transmitting communications over a network including instant messaging, virtual meetings and fax back.

Mitigation – Action to reduce the severity of risk (i.e. the probability or magnitude of the risk or both) or its actual or potential consequences, by implementing physical or technical security controls, or administrative or other business processes.

Mobile Device – Any computing system/device (e.g., laptop computer or wireless handheld device), that can create, receive, store, or transmit electronic information and is designed to be portable.

Network – A wired and/or wireless environment in which two or more computing systems/devices or medical devices are connected (e.g., through cables, waves, or infrared) in order to access, authenticate, share, transfer, transmit, or route information.

Network Connection – The connection between any computing system/device and a KP network. This includes but is not limited to connecting a computer or other device directly into the network via a cable, remote access (e.g. dial-in, broadband, etc.), or wireless.

Network Device – Hardware and supporting software used to manage network traffic or detect anomalies in network traffic; examples are routers, switches, firewalls, or intrusion detection/prevention devices, either wireless or wired.

Non-KP-Owned Computing Systems/Devices – Computing systems/devices that were not purchased or leased with KP funds.

Non-public Information – Any information KP has a duty to protect from the public:

- Under applicable law, e.g., protected health information (PHI), or
- Where KP is the custodian of data for a person who has a privilege under applicable law (e.g. psychotherapist-patient privilege, physician-patient privilege), or

- Per contract with another party, e.g., business information shared by or created with that party in connection with:
    - A business arrangement, e.g., purchase, or
    - A business function KP is performing on behalf of another organization, e.g., third party administrator; cardholder data.
- Non-public information also includes information that KP is entitled to protect from the public
    - By organizational choice, e.g., business plans and trade secrets, or
    - As privileged by law, e.g., peer review or attorney-client privileges.

Payment Application Data Security Standard (PA-DSS) – A standard developed by credit card companies that provide specifications for developing applications that process cardholder data (CHD). The goal of PA-DSS is to help software vendors and others develop secure payment applications that do not store prohibited data, such as full magnetic stripe, and ensure their payment applications support compliance with the PCI DSS.

Payment Card Industry Data Security Standard (PCI DSS) – Technical and operational requirements set by the Payment Card Industry Standards Council to protect cardholder data (CHD). The standards globally govern all merchants and organizations that store, process, or transmit this data. The goal of the PCI DSS is to protect cardholder data that is processed, stored, or transmitted by merchants.

Personal Email Accounts – Non-KP email accounts held by or available to covered individuals for personal or other use, or non-KP email accounts of vendors, business associates, or other persons who are not covered individuals.

Personally-owned Device (POD) – A medical or computing system/device (including laptops, workstations, personal data assistants, phones, cameras) or electronic storage media (including USB drives, CDs, DVDs, memory sticks, or any other media) that has the capability to capture or store information, and that is owned by a covered individual.

Policy – A Board of Directors or Senior Leadership statement directing the organization's thoughts and actions. Policies are used to integrate actions, information, and transaction flow across the organization. Policies promote consistent practices, compliance with applicable legal and regulatory requirements, and managing risk through effective controls.

Policy Owner – The department/national business function that leads the development of policy. The Policy Owner is accountable for the development of the policy document, and for identifying and/or engaging the individual(s) responsible for implementing and monitoring the policy.

Procedure – A sequence of specific events, tasks, or steps designed to complete a specific action. Procedures must be clear, unambiguous, and define expected outcomes.

Protected Health Information (PHI) – Individually identifiable information created, received or maintained by or on behalf of a covered health care provider or a health plan or other HIPAA covered entity. It includes individually identifiable information (oral, written, or electronic) that relates to (1) an individual's past, present, or future physical or mental health condition; (2) the provision of health care to an individual; or (3) past, present or future payment for the provision of health care to the individual. Only health information about an individual that is linked to that individual by an identifier is protected health information. Health information that is not linked to an individual by one or more of the 18 HIPAA identifiers and for which there is no reasonable basis to believe that the information can be used to identify the individual is not protected health information.

"HIPAA identifiers" means any of the following identifiers, either of the individual or of his/her relatives, employers or household members.

(1) Names

(2) All geographical 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, if according to the current publicly available data from the Bureau of the Census: (a) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (b) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000

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

(4) Telephone numbers

(5) Fax numbers

(6) Email addresses

(7) Social Security Numbers

(8) Medical record numbers

(9) Health plan beneficiary numbers

(10) Account numbers

(11) Certificate/license numbers

(12) Vehicle identifiers and serial numbers, including license plate numbers

(13) Device identifiers and serial numbers

(14) URLs

(15) Internet Protocol address numbers

(16) Biometric identifiers including finger and voice prints

(17) Full face photographic images and any comparable images; and

(18) Any other unique identifying number, characteristic, or code (provided that (a) the code or other record identifier is not derived from or related to other information (for example scramble MRNs and SSNs are not permitted) and not otherwise translatable to identify the individual; (b) the covered entity does not use or disclose the code or other record identifier for any other purpose; (c) and the covered entity does not disclose the mechanism for re-identification

Removal of all 18 HIPAA identifiers means the information is de-identified and no longer protected health information unless the covered entity has actual knowledge that the remaining information could be used alone or in combination with other information to identify an individual.

Not PHI – Identifiers that are not linked to an individual's health information are not protected health information. In addition, the disclosure of other identifiers or identifiable information in the possession of covered entities may be prohibited or limited without authorization under law unrelated to protections for protected health information. For example, Social Security numbers have California and federal privacy protection even when not linked to health information. Individually identifiable health information in KP employment records is not PHI; however, it may be subject to other state and federal privacy protections.

Remediation – To fix or correct process or control weaknesses or gaps.

Remote Access – The connection to a KP network or the KP Intranet initiated via dial-in, broadband, DSL, or other method, or an internal connection via modem (e.g., connecting via modem from a KP internal analog line).

Removable/Transportable Electronic Media – Magnetic, optical, or electronic storage media that are portable non-computing devices to which data can be downloaded and stored from a laptop or other endpoint computing device. Examples of such non-computing storage devices include, but are not limited to, CDs, flash memory drives, floppy disks, memory sticks, portable back-up devices, and mp3 players.

Residual Data – Any electronic data that remains stored on an endpoint computing system/device after completion of a task by an application or other software program. Residual data is not intentionally stored by the user and is retained by the system/device for restoring lost data, tracking user activity, and other background operations. The character strings that compose the data may or may not be decipherable or have meaning for a human being. Examples of residual data are temporary files, cached data, system logs, and Internet browser "cookies."

Risk – Risk is the probability that something may have a negative impact on business objectives given the potential impact of a threat and the likelihood of that threat occurring.

Risk Analysis – Analyzing and interpreting threats and vulnerabilities to networks, computing systems/devices, medical devices, electronic media, and KP information. Risk analysis includes assessment of the likelihood and impact of data integrity, availability or confidentiality being breached or compromised.

Risk Management – The culture, processes and workflow structures that are directed towards effective management of potential threats and vulnerabilities.

Risk Owner – Business manager/Business Application Owner with the authority to decide the treatment option for an identified risk.

Sarbanes-Oxley Act of 2002 (SOX) – Federal law requiring, among other things, public companies to report on the effectiveness of their internal controls, including but not limited to general controls over IT system acquisition, development, and implementation.

Safeguard – Protective measure to meet security requirements (i.e., confidentiality, integrity, and availability) for an information system. Safeguards may include technical, administrative, and physical constraints. Synonymous with *security control*.

Security Control – Protective measure to meet security requirements (i.e., confidentiality, integrity, and availability) for an information system. Security controls may include technical, administrative, and physical constraints. Synonymous with *safeguard.*

Security or Privacy Incident – An occurrence that may be intentional, accidental or inadvertent, which affects the confidentiality, availability, or integrity of KP non-public information or resources. Such occurrences include unauthorized modification or destruction of information or interference with computing or biomedical system/device operations. Examples of security or privacy incidents are:

- A breach of PHI as defined in the KP National Privacy and Security policy NATL.NCO.PS.025 Notifications Regarding Breaches of Protected Health Information.
- Infection of a KP system by a virus or other malicious software program.
- The acquisition by an unauthorized individual of identification and authentication credentials (e.g., ID badges, user IDs, passwords) that allows access to KP information or KP facilities/premises.
- Unauthorized access to KP networks or information systems, or the facilities that house them.
- Loss or theft of hardware containing KP confidential information (e.g., workstations, laptop computers, electronic media, hard drives, back-up tapes or devices).
- Erroneous mailing of member communications, including paper mailing, emailing, faxing, or other form of mail, such as FedEx.
- Fire or flood in a KP data center or on KP premises where electronic information may be compromised.
- Misuse of account privileges to gain access to resources not required to perform one's job duties.
- Denial of Service: When KP IT service availability or response-times degrade to an unacceptable level due to intentional interference or disruption.

Segregation of Duties – A key control that involves separating incompatible duties and/or responsibilities. Either manual or automated control to help prevent or decrease the risk of errors, irregularities, or fraud by ensuring no single individual has control over all phases of a transaction or business process.

Social Media – Includes but are not limited to blogs, podcasts, discussion forums, on-line collaborative information and publishing systems that are accessible to internal and external audiences (i.e., Wikis), RSS feeds, video sharing, and social networks like MySpace and Facebook.

SOX Financial Applications – Software and data used by KP the financial processes identified as subject to the requirements and controls of the Sarbanes-Oxley Act of 2002, whether supported by KP IT, the business, or a third party service provider.

Spyware – Any software that covertly gathers user information through the user's Internet connection without his or her knowledge. Once installed, spyware monitors user activity on the Internet and transmits information about the activity in the background to another party. Spyware is most often used to gather information about email addresses, passwords, credit card numbers, and other personal information.

Storage – Retaining information in an electronic format, e.g., on a network server, a workstation, mobile device, or optical or magnetic medium (e.g. internal memory or hard drive, CD, tape, flash drive).

Strong Password – A password that is difficult for both individuals and computer programs to decode and that helps to protect data from unauthorized access.

Structured Information – Information whose components are similar, have a common taxonomy, and which can be queried. Examples include forms, spreadsheets, and documents.

Taxonomy – The organization of information elements according to a defined nomenclature and structure.

Technical Safeguards – The technology (e.g., anti-virus software) and the policy and procedures for its use that protect and/or control access to electronic information.

Third Party – Vendors or other non-KP entities accessing KP networks for purposes of maintenance, monitoring, problem solving, or upgrading an application, system, or other computing device.

Threat – The potential for a person or thing to execute a specific vulnerability through accidental or intentional means.

Two-factor Authentication – Verification of the identity of a person, process, or a computing system/device, by at least two of the following: passwords, tokens, or biometrics (e.g., fingerprints, retina scans).

Unstructured Information – Information whose component pieces of data may be very dissimilar, does not have a common taxonomy, and which is not easily queriable. Examples include images and email messages.

User ID/Account – Character string used to uniquely name an individual, group, or automated process. The combination of a user ID/account and another identifier such as a password authenticates the individual/group or process to computing systems/devices or medical devices at the authorized level of access.

Virtual Meetings – Real time electronic meetings created, simulated or carried out utilizing computers and computer networks to facilitate communication among geographically dispersed covered individuals and/or third parties. Virtual meetings do not include telemedicine encounters, the use of health care information exchanged from one site to another via electronic communications for the health and education of the patient or health care provider, and for the purpose of improving patient care, treatment, or services.

Vendor – Any individual or organization that offers, supplies, or sells products or services to KP, including independent contractors such as consultants.

Virus or Other Malicious Software Program – A computer program that, when executed, damages a computing system/device, network, and/or information, results in reduced availability of information technology resources or gathers information about the user. Examples of damage include simple nuisance messages; deletion of hard drive information; providing computer or network access to attackers; crippling network servers through a flood of network traffic; and capturing passwords, email lists, and other information. Examples of malicious software programs include viruses, worms, Trojan horses, and spyware.

Vulnerability – A flaw or weakness in design, procedure, implementation, or controls that could be executed accidentally or by intentional means, and results in a security incident or non-compliance with KP's policies and procedures.

Wireless – Term used to describe any computer network or device where there is no physical wired connection between sender and receiver and communications are maintained by radio waves and/or microwaves.

Wireless Handheld Device – Refers to cellular telephones, pagers, personal digital assistants, (PDAs) and other wireless handheld data and communication devices, including associated accessories such as cellular modems and adapters. A Wireless Handheld Device may have one or multiple functions and each is accompanied with wireless service that sets forth the allowable minutes for airtime and roaming, data allocations for email and web browsing. The definition of Wireless Handheld Devices specified herein may be modified to address changes in technology. Any new features and functionality that augment or enhance Wireless Handheld Devices will be subject to [the KP policy *Use of Wireless Handheld Devices*, NATL.HR.024.]