Policy Title: Obligations Regarding Confidentiality	Policy Number: REGL.HR.001a
Owner Department: Human Resources	Effective Date: 7/2/14
Custodian: HR Compliance	Page: 1 of 4

1.0 Policy Statement

Employees are required to protect confidential patient, member, personnel and business information from unauthorized access, use or disclosure.

2.0 Purpose

The purpose of this policy is to establish employees' confidentiality obligations.

3.0 Scope/Coverage

This policy applies to all employees in regions outside of California* who are employed by any of the following entities (collectively referred to as "Kaiser Permanente"):

3.1 Kaiser Foundation Health Plan, Inc. and Kaiser Foundation Hospitals (together, KFHP/H); and

3.2 KFHP/H's subsidiaries.

*Regions outside of California are Colorado, Georgia, Hawaii, MidAtlantic, and Northwest. This policy also applies to employees in National Functions who work in regions outside of California.

4.0 Definitions

4.1 **Confidential and/or Restricted Business information:** KP records or information in any form (verbal, written or electronic) related to business plans and strategies (including service, marketing, member, licensing and purchase agreements), financial status and projections, customer accounts, intellectual property (e.g., inventions, trade secrets) member rates and benefits, technical data or drawings, audits, legal documents and communications, and any other records and information that are marked as confidential and/or proprietary (e.g., business concepts, strategies and plans, clinical and financial data, intellectual property, reports, and report formats). (See Information Security Policy NATL.IS.001: 03.0 *Security Requirements for Information Management*.)

4.2 **Confidential Personnel information**: KP information in any form (verbal, written, electronic) that is related to the status of an employee and that uniquely identifies the employee(e.g., social security numbers, personnel files and records related to corrective/disciplinary action, performance, compensation, transfer, promotion, benefits and other terms and conditions of employment). Personnel-related information (e.g., social security numbers) pertaining to contingent workers is also considered confidential. An individual employee is not required to maintain confidentiality of personnel information that specifically pertains to that employee.

4.3 **Protected Health Information (PHI)**: Individually identifiable health information as defined in KP Privacy and Security policies. Individually identifiable health information in KP employment records is not PHI; however, it is considered Confidential Personnel Information. (Additional definitions related to

PHI, including "access", "disclosure", and "use" can be found in KP's Privacy and Security policies.)

5.0 Provisions

5.1 Confidentiality Agreement

5.1.1 As part of the new hire process, employees are issued a copy of KP's Principles of Responsibility and are required to sign a Confidentiality Agreement as a condition of employment.

5.1.2 Employees may also be required to re-sign a Confidentiality Agreement in accordance with regional and/or credentialing requirements.

5.1.3 In addition to the Confidentiality Agreement, employees may be requested to sign non-disclosure agreements (NDAs) under certain circumstances.

5.1.4 Independent contractors must comply with confidentiality obligations as stipulated in their contracts with KP. Consultants must comply with the nondisclosure requirements in their engagement contracts. Contingent workers (see NATL.HR.035, Contingent Workers) must comply with the confidentiality obligations stipulated by the region in which they work.

5.2 Prohibited Conduct

5.2.1 In accordance with the Minimum Necessary Privacy policy, employees are limited to the minimum necessary when accessing, using and disclosing PHI to perform their assigned job duties.

5.2.2 An employee who does not need to access, use or disclose a particular individual's PHI in order to perform his/her job duties (including a minor child, other family member, friend or third party) must obtain, prior to the access, a written authorization from the individual (as applicable), and must follow the same procedures that apply to non-employee health plan members in order to obtain another person's PHI. (See NATL.NCO.PRIV.018, Personal Representatives.) Written authorization from that individual does not convey authority to directly access electronic, paper, or hybrid medical records, or any other KP records containing PHI.

5.2.3 Employees may only access their own PHI by following the same procedures that apply to non-employee health plan members, (e.g., through kp.org). (See NATL.NCO.PRIV.001, Access to Protected Health Information by Members and Patients.)

5.2.4 An employee may not add, change, delete, remove or destroy any information from an electronic, paper, or hybrid medical record unless authorized as part of his/her job duties. Falsifying medical information is prohibited.

5.2.5 Access, use or disclosure of Confidential and/or Restricted Business Information, Confidential Personnel Information, or PHI that is not necessary to perform assigned job duties, or that is otherwise in violation

of this policy, is subject to corrective/disciplinary action, up to and including termination of employment. The level of corrective/disciplinary action will depend on the type of violation and the conduct of the employee, and will be consistent with any applicable KP policies, collective bargaining agreements and privacy and security laws and regulations. An employee who violates laws protecting confidentiality of information or the privacy rights of others may also be subject to criminal prosecution or a civil lawsuit for penalties and/or economic harm.

5.2.6 Disclosures of business information to financial market professionals or public audiences must be in accordance with Internal and External Financial Communications NATL.FIN.ACCT.16.F. Disclosures of business information in conjunction with outsourcing KFH/HP business to third parties must be in accordance with Outsourcing Financial Transaction Processing NATL.FIN.ACCT.15.F.

5.2.7 Employees must comply with KP policies that protect the security and confidentiality of Business and/or Restricted Information, Personnel Information, and PHI. For example, employees are prohibited from sharing logons and passwords and using other employees' logons and passwords, unless failure to do so would pose a significant risk to patient care (see Information Security Policy NATL.IS.001: 12.0 User Access Management.).

5.3 Continuing Confidentiality Obligation upon Termination of Employment

5.3.1 After they resign or terminate their employment with KP, employees are obligated to continue to maintain the confidentiality of all Business and/or Restricted Information, Personnel Information, and PHI they learned or had access to during their employment. They must return all records (originals and copies) and equipment, including applicable information maintained in electronic form containing Confidential and/or Restricted Business Information, Confidential Personnel Information, or PHI to their supervisor no later than the last day of work.

5.3.2 Supervisors must ensure that the terminated employee's access to Confidential and/or Restricted Business Information, Confidential Personnel Information, and PHI is discontinued, including revocation of logon IDs, systems access codes and/or passwords as required by NATL.HR.013, Processing Employee Terminations.

5.4 Reporting Confidentiality Loss, Theft or Other Unauthorized Disclosure

5.4.1 Employees must promptly report any suspected loss, theft, or other incidents of unauthorized disclosure of confidential information (e.g., if a mobile computing device is stolen or there is evidence that someone is using their password) to their supervisor, other management, HR representative, Compliance/Privacy Officer or the KP Compliance Hotline. Failure to report these incidents may result in corrective/disciplinary action, up to and including termination.

5.4.2 Supervisors are obligated to promptly report suspected loss, theft, or other incidents of unauthorized disclosure of confidentiality to their local

Compliance/Privacy Officer in accordance with national/regional policies and procedures. Failure to report these incidents may result in corrective/disciplinary action, up to and including termination.

5.4.3 KP will report unauthorized access, use or disclosures of protected health information to a governmental agency if such reporting is required by state or federal laws and regulations. Such required reporting may include names of the employees responsible for unauthorized access, use or disclosure, which may result in governmental actions against individuals in the form of civil, criminal, or licensor actions.

6.0 References/Appendices

6.1 NATL.IS.001: 03.0 *Security Requirements for Information Management*

6.2 NATL.HR.035, *Contingent Workers*

6.3 NATL.NCO.PRIV.014, *Minimum Necessary*

6.4 NATL.NCO.PRIV.018, *Personal Representatives*

6.5 NATL.NCO.PRIV.001, *Access to Protected Health Information by Members and Patients*

6.6 NATL.FIN.ACCT.16.F, *Internal and External Financial Communications*

6.7 NATL.FIN.ACCT.15.F, *Outsourcing Financial Transaction Processing*

6.8 NATL.IS.001: 12.0 *User Access Management*

6.9 NATL.HR.013, *Processing Employee Terminations*

7.0 Approval

Update approval, 7/2/14

In accordance with the charter of the National HR Policy Roundtable, this policy update was approved by the National HR Policy Roundtable members, as chaired by Francie Sloan.

Policy Life History

Original Approvals	Update Approvals	Revision Approvals
Approval Date: 4/5/10	**Approval Date: 4/26/12; 7/2/14**	**Approval Date: n/a**
Effective Date: 4/5/10	**Effective Date: 4/26/12; 7/2/14**	**Effective Date: n/a**
Communicated Date: n/a		**Communicated Date: n/a**