KERN HEALTH SYSTEMS

KERN HEALTH SYSTEMS POLICY AND PROCEDURES			
Policy Title	Protected Health Information (PHI) Privacy, Use, and Disclosure	**Policy #**	14.03-P
Policy Owner	Compliance	**Original Effective Date**	08/29/1997
Revision Effective Date	01/01/2024	**Approval Date**	05/29/2025
Line of Business	☒ Medi-Cal ☐ Medicare ☐ Corporate		

I. PURPOSE

To establish the policy and procedures for the receipt, access, use, disclosure, maintenance, disposal, and security of confidential and protected health information.

II. POLICY

Kern Health Systems (KHS) employees, subcontractors, and providers are required to comply with applicable portions of the Confidentiality of Medical Information Act (California Civil Code §56 through §56.37) and the Health Insurance Portability and Accountability Act ("HIPAA") (United States Code of Federal Regulations Title 45 Parts 160 and 164).

Kern Health Systems (KHS) employees may not receive, access, use or disclose Protected Health Information (PHI) except as permitted or required by this Policy and Procedure and applicable State and Federal regulations. Except to the extent expressly authorized by the patient or to the extent permitted or required by this Policy and Procedure and by applicable State and Federal regulations, neither KHS nor its contracted practitioners/providers shall intentionally share, sell, or otherwise use any medical information for any purpose not necessary to provide health care services to the patient.

Telecommuting or on-worksite, confidential patient information will be created (including print version), maintained, preserved, stored, abandoned, destroyed, and disposed of in a manner that preserves the confidentiality of the information and prevents its retrieval in any individually identifiable form by any unauthorized person or entity.

The Chief Compliance and Fraud Prevention Officer will serve as KHS's Privacy Official, supported by the Director of Compliance and Regulatory Affairs and designated compliance department staff. Compliance is responsible for the development and implementation of privacy policies and procedures.

III. DEFINITIONS

TERMS	DEFINITIONS
Authorized Representative	Any individual appointed in writing by a competent Member or Potential Member, to act in place or on behalf of the Member or Potential Member for purposes of assisting or representing the Member or Potential Member with Grievances and Appeals, State Fair Hearings, Independent Medical Reviews, and in any other capacity, as specified by the Member or Potential Member.
Breach	A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual. (Exceptions to a breach may exist).
Business Associate	A person who: A. performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information, including but not limited to claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management B. provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services where the provision of services involves the disclosure of individually identifiable health information KHS employees are not considered business associates of KHS. Other covered entities may also be considered business associates of KHS.
Cloud S	Includes any online service that allows storage of data to be stored outside of KHS's network
Confidential Communications Request	A request by a subscriber or enrollee that health care service plan communications containing medical information be communicated to them at a specific mail or email address or specific telephone number, as designated by the subscriber or enrollee
Confidential Information	Facts, documents, or records in any form that are recognized as "confidential" by any law, regulation, or contract
Covered Entity	Entities that must comply with HIPAA regulations. Covered entities include: (1) health plans; (2) health plan clearinghouses; or (3) health care providers who transmit any health information in electronic form in connection with a transaction covered by HIPAA.
Covered Functions	Those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.
Disclosure	The release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information, as defined in § 160.103, Title 45, of the Code of Federal Regulations

Gender Affirming Health Care	Medically necessary health care that respects the gender identity of the patient, as experienced and defined by the patient, and may include, but is not limited to, the following: A. Interventions to suppress the development of endogenous secondary sex characteristics. B. Interventions to align the patient's appearance or physical body with the patient's gender identity. C. Interventions to alleviate symptoms of clinically significant distress resulting from gender dysphoria, as defined in the Diagnostic and Statistical Manual of Mental Disorders, 5th Edition.
Gender Affirming Mental Health Care	Mental health care or behavioral health care that respects the gender identity of the patient, as experienced and defined by the patient, and may include, but is not limited to, developmentally appropriate exploration and integration of identity, reduction of distress, adaptive coping, and strategies to increase family acceptance.
Health Care Operations	Any of the following activities of the covered entity to the extent that the activities are related to covered functions: A. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such 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 with information about treatment alternatives; and related functions that do not include treatment B. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, 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 C. Underwriting, premium rating, 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 claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of 45 CFR§164.514(g) are met, if applicable D. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs E. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development, or improvement of methods of payment or coverage policies; and

	F. Business management and general administrative activities of the entity, including but not limited to: 1. Management activities relating to implementation of and compliance with the requirements of this subchapter 2. Customer service, including the provision of data analyses for policy holders, plan sponsors, or their customers, provided that PHI is not disclosed to such policy holder, plan sponsor, or customer 3. Resolution of internal grievances 4. The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and 5. Consistent with the applicable requirements of 45 CFR §164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.
Health Oversight Agency	An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant
HIPAA	The Health Insurance Portability and Accountability Act. United States Code of Federal Regulations Title 45 Parts 160 and 164.
HITECH	Health Information Technology for Economic and Clinical Health (HITECH) Act requiring HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.
Individually identifiable health information	Medical information that includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity. Individually identifiable health information also includes race/ethnicity, language, gender identity, and sexual orientation information.
Medical information	Any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental health application information, reproductive or sexual health application information, mental or physical condition or treatment. "Individually identifiable" means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the

	individual's identity (as defined in Civil Code section 56.05, subdivision (j)). Medical information also includes race/ethnicity, language, gender identity, and sexual orientation information.
Medical Records	The record of a member's medical information, including but not limited to medical history, care or treatments received, test results, diagnoses, and prescribed medications.
Mental Health Application Information	Information related to a consumer's inferred or diagnosed mental health or substance use disorder, as defined in Section 1374.72 of the Health and Safety Code, collected by a mental health digital service.
Mental Health Records	Patient records, or discrete portions thereof, specifically relating to evaluation or treatment of a mental disorder. This includes, but is not limited to, all alcohol and drug abuse records.
Mobile Device	Includes any non-fixed device containing an operating system that may be used to create, access, or store SEI (i.e., laptop computers, tablet computers, smart phones, etc.)
Payment	A. The activities undertaken by: 1. A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or 2. A covered health care provider or health plan to obtain or provide reimbursement for the provision of health care; and B. The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to: 1. Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims. 2. Risk adjusting amounts due based on enrollee health status and demographic characteristics 3. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing 4. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges 5. Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and 6. Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement: i. Name and address ii. Date of birth iii. Social security number iv. Payment history

	v. Account number vi. Name and address of the health care provider and/or health plan
Protected Health Information (PHI)	Individually identifiable health information that is transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium. Protected Health Information also includes race/ethnicity, language, gender identity and sexual orientation information.
Protected Individual	Any adult covered by the subscriber's health care service plan or a minor who can consent to a health care service without the consent of a parent or legal guardian, pursuant to state or federal law. "Protected individual" does not include an individual that lacks the capacity to give informed consent for health care pursuant to Section 813 of the Probate Code.
Provider	A physician, nurse, nurse mid-wife, nurse practitioner, medical technician, physician assistant, hospital, laboratory, ancillary provider, or other person or institution that furnishes Covered Services.
Psychotherapist	A person who is both a psychotherapist as defined in Section 1010 of the Evidence Code *and* a "provider of health care" as defined in the Health and Safety Code. This means the provider must meet both tests. Section 1010 defines a psychotherapist to include psychiatrists, psychologists, clinical social workers, marriage, family and child counselor, and other professionals who provide mental health care or the person authorized or reasonably believed by the patient to be authorized to practice psychiatry.
Psychotherapy Notes	Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. This excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.
Reproductive or sexual health application information	Information about a consumer's reproductive health, menstrual cycle, fertility, pregnancy, pregnancy outcome, plans to conceive, or type of sexual activity collected by a reproductive or sexual health digital service, including, but not limited to, information from which one can infer someone's pregnancy status, menstrual cycle, fertility, hormone levels, birth control use, sexual activity, or gender identity.
Reproductive or sexual health digital service	A mobile-based application or internet website that collects reproductive or sexual health application information from a consumer, markets itself as facilitating reproductive or sexual health services to a consumer, and uses the information to facilitate reproductive or sexual health services to a consumer.
Sensitive Services	All health care services related to mental or behavioral health, sexual and reproductive health, sexually transmitted infections, substance use disorder, gender affirming care, and intimate partner violence, and includes services described in Sections 6924, 6925, 6926, 6927, 6928, 6929, and 6930 of the Family Code, and Sections 121020 and 124260 of the Health and Safety Code, obtained by a patient at or above the minimum age specified for consenting to the service specified in the section (as defined in Civil Code section 56.05, subdivision (p)).

Sensitive Electronic Information (SEI)	Includes all classes of sensitive data including Protected Health Information (PHI) and any other information considered confidential by the organization. Sensitive Electronic Information (SEI) also includes race/ethnicity, language, gender identity, and sexual orientation information.
Use	Has the meaning in Section 160.103 of Title 45, Code of Federal Regulations: including the following: the sharing, employment, application, utilization, examination, or analysis of the PHI within an entity that maintains such information.

IV. PROCEDURES

A. Protected Health Information (PHI) Policies and Procedures

1. KHS implements policies and procedures with respect to PHI that are designed to comply with HIPAA regulations and the DHCS Contract. These policies and procedures are changed as necessary and appropriate to comply with changes in the law.

2. Each network provider must implement and maintain the following:

    a. Procedures for storage and filing of medical records including collection, processing, maintenance, storage, retrieval identification, and distribution.

    b. A written policy to protect medical records from loss, tampering, alteration, destruction, and to maintain confidentiality in accordance with Federal and State law.

    c. A written procedure for the release of information and obtaining consent for treatment.

    d. Documentation of the titles of persons responsible for receiving and processing requests for amendments by individuals.

B. Protected Health Information (PHI) Identifiers

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 specifies a number of elements in health data that are considered identifiers. If any are present, the health information cannot be released without patient authorization.

1. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial 3 digits of a zip code, if according to the current publicly available data from the Bureau of the Census

2. The geographic unit formed by combining all zip codes with the same 3 initial digits contains more than 20,000 people; and

3. The initial 3 digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000. 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 such ages and elements may be aggregated into a single category of age 90 or older

4. Telephone numbers

5. Fax numbers

6. Electronic mail 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. Web Universal Resource Locators (URLs)

15. Internet Protocol (IP) address numbers

16. Biometric identifiers, including finger and voice prints

17. Full face photographic images and any comparable images

18. Any other unique identifying number, characteristic, or code, including race/ethnicity, language, gender identity and sexual orientation data.

C. Confidential Information

1. KHS has the following duties and responsibilities with respect to confidentiality of information and data:

   a. Notwithstanding any other provision of the DHCS contract, names of persons receiving public social services are confidential and are to be protected from unauthorized disclosure in accordance with 42 CFR section 431.300 et seq., W&I Code section 14100.2, and regulations adopted thereunder.

b. For the purpose of the DHCS Contract, all information, records, data, and data elements collected and maintained for the operation of the contract and pertaining to members will be protected by KHS.

c. KHS may release Medical Records in accordance with applicable law pertaining to the release of this type of information. KHS is not required to report requests for Medical Records made in accordance with applicable law.

2. KHS, and our Subcontractors, Downstream Subcontractors, or Network Providers, concerning a member under the DHCS Contract, KHS will ensure the following for any identifiable information obtained:

a. Any such information will not be used for any purpose other than conducting the express terms of the DHCS Contract.

b. All requests for disclosure of such information will be promptly transmitted to DHCS, except requests for Medical Records in accordance with applicable law.

c. Any such information will not be disclosed, except as otherwise specifically permitted by the DHCS Contract, to any party other than DHCS without DHCS' prior written authorization specifying that the information is releasable under 42 CFR section 431.300 *et seq.*, W&I Code section 14100.2, and regulations adopted thereunder; and

d. At the termination of the DHCS Contract, the return all such information to DHCS or maintain such information as directed by DHCS.

e. KHS will have provisions in its Subcontract Agreements and Network Provider Agreements requiring Subcontractors, Downstream Subcontractors, and Network Providers to comply with these requirements.

f. KHS will have policies and procedures in place to ensure Members' rights to confidentiality of PHI and PI in accordance with 45 CFR Parts 160 and 164, and in accordance with Civil Code section 1798 et seq. KHS will:

i. Ensure that all Subcontractors, Downstream Subcontractors, and Network Providers have policies and procedures in place to guard against unlawful disclosure of PHI, PI, and any other Confidential Information to any unauthorized persons or entities.

ii. Inform and advise Members on the right to confidentiality of their PHI and PI.

iii. Obtain the Member's prior written authorization to release Confidential Information, unless such prior written authorization is not required by 22 CCR section 51009.

3. KHS, our employees, agents, or subcontractors will:

    i. Protect from unauthorized disclosure names and other identifying information concerning persons either receiving services pursuant to the DHCS agreement or persons whose names or identifying information become available or are disclosed to KHS, our employees, agents, or subcontractors as a result of services performed under the agreement, except for statistical information not identifying any such person.

    ii. Not use such identifying information for any purpose other than carrying out KHS' obligations. Promptly transmit to the DHCS Program Contract Manager all requests for disclosure of such identifying information not emanating from the member outside of disclosures allowed for treatment, payment, and healthcare operations or required by law.

4. KHS will not disclose, except as otherwise specifically permitted or authorized by the member, any such identifying information to anyone other than DHCS without prior written authorization from the DHCS Program Contract Manager, except if disclosure is allowable or required by State or Federal law.

5. For purposes of this provision, identity shall include, but not be limited to name, identifying number, symbol, or other identifying data assigned to the individual, such as finger or voice print or a photograph.

6. As deemed applicable by DHCS, this provision may be supplemented by additional terms and conditions covering personal health information (PHI) or personal, sensitive, and/or confidential information (PSCI).

D. Member Rights Regarding Protected Health Information

As members of Kern Family Health Care (KFHC), our members have the following rights. Additional information on these rights can be found throughout this policy, in the member handbook, and in the Notice of Privacy Practices.

1. Right to Confidentiality

2. Right to request restrictions for how PHI is used or disclosed

3. Right to request PHI be amended

4. Right to be notified in case of a breach or unsecured protected health information

5. Right to authorize others to get PHI on the member's behalf

6. Right to request confidential communications

7. Right to access the member's own PHI

8. Right to receive an accounting of non-routine disclosures

E. Restrictions on Use and Disclosure

1. The member or a member's Personal Representative can request to restrict either the Use and/or Disclosure of the member's PHI, but KHS may not agree to such restrictions.

2. Request for restrictions must be submitted in writing and include:

    a. The PHI that is to be restricted

    b. Whether the member wants to restrict the Use, Disclosure, or both; and

    c. To whom the limitations apply (e.g., Disclosures to a spouse)

    d. KHS will discuss the request with the member or a member's Personal Representative to ensure that such restrictions are in the member's best interest.

    e. KHS will advise the member that KHS:

        i. Retains the right to approve or deny such request

        ii. May release the restricted PHI in emergency situations

        iii. May release the restricted PHI if Required by Law; and

        iv. May terminate the agreement to restrict PHI.

    f. KHS will review a member's request to restrict Use and Disclosure of PHI in coordination with Business Associates, as appropriate.

    g. KHS will document the restriction, if any.

    h. KHS must notify the member of the decision to approve or deny the member's request within thirty (30) calendar days of receipt of the request.

    i. KHS may terminate its agreement to a restriction of Use and Disclosure under the following circumstances:

        i. The member agrees to, or requests, the termination, in writing.

        ii. The member agrees verbally to the termination, and the verbal agreement is documented by KHS.

        iii. KHS notifies the member that it shall terminate its agreement to the restriction(s), except that such termination is only effective with respect to PHI created, or received, after the individual has been notified of the termination.

j. KHS will retain copies of all requests and related notices on file for ten (10) years from the date the request is received by KHS or the date when the restriction was last in effect, whichever is later.

F. Amendments to PHI

KHS, and our subcontractors and contracted providers, must act on the individual's request for an amendment no later than sixty (60) days after such a request.

1. Denied Amendments

a. We may deny an individual's request for amendment if it determines that the PHI:

i. Was not created by us, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment.

ii. Qualifies as PHI to which the individual can be denied access to inspection.

iii. Is accurate and complete.

b. The covered entity must provide a written denial. The denial must use plain language and contain the following elements:

i. The basis for the denial.

i. The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement.

ii. A statement that if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment.

iii. A description of how the individual may complain to the covered entity or to the Secretary of the United States Department of Health and Human Services. The description must include the name/title and telephone number of the covered entity's appropriate contact person.

iv. Upon receipt of a written statement of disagreement from the member, the covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered entity must provide a copy to the individual.

2. Accepted Amendments:

a. KHS, our subcontractors and/or network providers will make the appropriate amendment to the PHI by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

b. The covered entity must inform the individual that the amendment is accepted and obtain the individual's identification of an agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared including:

i. Persons identified by the individual as having received PHI about the individual and needing the amendment.

ii. Persons, including business associates, that the covered entity knows have the PHI that is the subject of the amendment and that may have relied, or could foreseeably rely on such information to the detriment of the individual.

G. Access to Protected Health Information

1. Password Policy

   KHS requires the establishment of unique employee-specific usernames and passwords to access PHI.

   a. KHS employees are prohibited from sharing username and password information with anyone.

   b. KHS enforces a password policy that consists of the following:

      i. Password must be at least 14 characters in length

      ii. Contain characters from three of the following four categories:

      iii. English uppercase characters (A through Z)

      iv. English lowercase characters (a through z)

      v. Base 10 digits (0 through 9)

      vi. Contain special characters !@#$%^&*()_+

2. Role-based Access Control

   Based on the assigned position of each employee, a role-based permission is assigned, which allows the employee to access data and perform only the tasks authorized to perform as part of his/her job functions.

3. PHI may be stored and/or accessed through different types of devices and media, provided appropriate approvals are obtained and security protocols have been followed. The devices and media that may be impacted include but are not limited to:

    a. Desktop Computers

    b. Laptop Computers

    c. Removable media as defined below

4. Access to KHS Data Storage

    Sensitive Electronic Information (SEI) data will be stored at authorized data storage locations. (Contact the KHS Help Desk for a list of authorized data storage locations).

    a. Access to KHS data storage is protected by unique user accounts, which are assigned to a role-based access control that enforces SEI to be protected from unauthorized access.

    b. All access to SEI data is audited and reviewed for analysis for any potential signs of abuse and/or unauthorized access.

    c. Only approved cloud storage providers are authorized to store and transfer SEI data. (Contact the KHS Help Desk for a list of authorized cloud storage providers).

5. New Employees, Internal Transfers, Promotions

    Upon a KHS employee being hired initially or assigned to a new position/role, the following work will be performed:

    a. KHS' Human Resource department notifies the KHS Help Desk of the new position/role by opening a Help Desk ticket. Including the employee's new position/role at KHS.

        i. Human Resources coordinates with the hiring manager to complete a New Employee System Request Form (NESR), which specifies the hardware, applications/systems, workflows, building access, email distribution lists, etc. to which the new employee requires access.

    b. The Help Desk technician makes the necessary changes to the employee's account, including but not limited to:

        i. If necessary, delegating the required work to the appropriate System Administrator of the system for which the employee needs access.

ii. Removing/terminating previous role-based permissions to ensure the employee only has the required permissions to access data/systems and perform functions specific to the new position/role at KHS.

c. Once the work is completed and documented on the Help Desk ticket, the employee's manager/supervisor is notified the required work has been completed.

6. Employee responsibility changes without a position change/transfer

Should an employee's responsibilities in the current position change and the employee requires access to new systems or data, or no longer requires access to a specific system or subcomponent of the system, the following work will be performed:

a. The employee's manager must notify the KHS Help Desk of the change of access to the specific system by opening a Help Desk ticket.

b. The Help Desk technician makes the necessary changes to the employee's account, including but not limited to:

i. If necessary, delegating the required work to the appropriate System Administrator of the system for which the employee needs access.

ii. Removing/terminating previous role-based permissions to ensure the employee only has the required permissions to access data/systems and perform functions specific to the new position/role at KHS.

c. Once the work is completed and documented on the Help Desk ticket, the employee's manager/supervisor is notified that the required work has been completed.

7. Termination of access for KHS employees

KHS ensures employee terminations, including voluntary and involuntary terminations, and terminations due to the death of an employee, are handled professionally with minimal disruption to the workplace. (Voluntary = Notice provided; employment and access ends at an agreed upon date and time; Involuntary = Employment and access is immediately terminated.

a. Upon a KHS employee's access being terminated due to voluntary separation, the following work will be performed:

i. KHS' Human Resources department will notify the KHS Help Desk of the termination by opening a Help Desk ticket, including the date and time the KHS employee's access will need to be terminated.

ii. The Help Desk technician will make the necessary changes to the employee's account to ensure access to KHS data, information, and systems is removed/terminated; if necessary, delegating the required work to the appropriate System Administrator of the systems to which the employee had access.

b. Upon a KHS employee's access being terminated due to involuntary separation, the following work will be performed:

i. KHS' Human Resources department will verbally notify the KHS Help Desk of the termination and open a Help Desk ticket.

ii. The Help Desk technician will immediately disable the employee's account; if necessary, delegating the required work to the appropriate System Administrator of the systems to which the employee had access.

H. Safeguards

1. KHS, our subcontractors, and our providers are required to employ a variety of safeguards to ensure protected health information is secure. KHS has implemented many administrative, physical, and technical safeguards, including but not limited to those outlined throughout this policy and the following:

   a. HIPAA and Security training is required upon hire and annually thereafter.

   b. Employees, subcontractors, and providers are subject to disciplinary standards, up to and including termination, for failing to comply with HIPAA, privacy, and confidentiality requirements.

   c. Reinforcement of expectations related to HIPAA and PHI through the *KHS Code of Conduct*, *Compliance Program*, and *Compliance Guide*.

   d. Requiring business associate agreements with our subcontractors, as outlined within *14.61, Delegation Policy*.

   e. Security management systems and processes in place for preventing, identifying, and resolving any system compromises, such as cyber-attacks or malware, and unauthorized access.

   f. Maintaining Contingency and Disaster Recovery Plans

   g. Facility and access controls, including but not limited to the use of security guards and security cameras; limiting access to the building; specific processes for accepting visitors; the use of photo identification badges, which also requires swiping the badge to not only enter the building, but areas within the building, etc.

   h. Workstation security through the use of user-specific logon credentials, activity monitoring, and system time outs.

I. Protection and security of PHI

KHS employees, subcontractors, and providers have an obligation and are required to protect medical information, PHI, PI, and EPHI as outlined within all regulatory requirements, the trainings provided, and this policy. Those who create, maintain, preserve, or store patient medical information must do so in a manner that preserves the confidentiality of the information and prevents its retrieval in any individually identifiable form by any unauthorized person or entity. Additional responsibilities include, but are not limited to:

1. The security of records that are only maintained in electronic form, including providers that utilize electronic recordkeeping systems only, must comply with the additional requirements of California Health and Safety Code §123149 as appropriate.

2. Appropriate safeguards shall be diligently followed regarding securing PHI or Personally Identifiable Information ("PII") at an off-site location. PHI/PII must be secured in a manner so that it cannot be accessed by unauthorized individuals.

3. An individual within the provider's office must be assigned the responsibility of securing and maintaining medical records at each network provider office.
4. Appropriately storing any paper which contains PHI

    a. Ensure paper is not face up at workstations

    b. Lock PHI in filing cabinets

5. Lock computer screens when leaving a workstation.

6. Use encryption for emails containing ePHI.

7. Use Secure File Transfer Protocols (SFTP) for sending PHI.

8. Do not discuss PHI outside of work under any circumstances.

9. Protect PHI on computers, laptops, copy machines, or other electronic devices.

10. When faxing member information, double-check the recipient's number.

11. Immediately retrieve any printouts or copies containing PHI from copy machines/printers.

12. Do not leave passwords exposed.

13. Reporting any violation of this policy to an immediate supervisor, the Compliance HIPAA email node (HIPAATeam@khs-net.com), the Chief Compliance Officer, or Director of Compliance. Anonymous reports may also be made through the Ethics Hotline.

J. Disposal of Protected Health Information

1. Telecommuting or on-worksite, KHS employees and providers who abandon, destroy, or dispose of medical information, must do so in a manner that preserves the confidentiality of the information and does not allow for retrieval of any individually identifiable form by any other person or entity.

2. Disposal or destruction must be complete and thorough. Any paper or printed material containing confidential information must be thoroughly shredded prior to disposal.

3. Medical records must be kept for a minimum of ten (10) years, except for minors whose records must be kept at least until one year after the minor has reached the age of 18, but in no case less than ten (10) years.

K. Data and Hardware Disposal

KHS requires that all KHS electronic devices be destroyed or decommissioned prior to being recycled, sold, or donated.

1. KHS employees must contact the KHS Help Desk when a KHS owned and/or leased electronic device (Ex. Printers, PCs, tablets, etc.) requires disposal and subsequently follow the Help Desk's instructions on pickup/delivery of the electronic device(s).

2. KHS Help Desk Technicians will perform the following when disposing of an electronic device:

    a. Coordinate with KHS employee for pickup of electronic device(s).

    b. Follow the KHS Data and Hardware Disposal procedure.

3. The Director of IT Operations is responsible for ensuring that the KHS Data and Hardware Disposal Procedures are implemented and enforced by all KHS departments.

4. The supervisor of KHS Help Desk is responsible for:

    a. Ensuring proper disposal of data and hardware from KHS owned and/or leased electronic devices by following the KHS Data and Hardware Disposal procedures.

    b. Reporting to the Director of IT Operations on any violation of this policy regarding the KHS Data and Hardware Disposal.

L. Devices and Removable Media

By default, KHS restricts the use of all removable media on all KHS devices. KHS employees are responsible for securing mobile and removeable devices in alignment with the below:

1. Use of removable media must be approved by the Chief Information Officer (CIO).

2. Removable media must be issued by the KHS Help Desk, if approved.

    a. Types of removable media include:

        i. CDs/DVDs

ii. External hard drives

iii. USB flash drives (thumb drives)

3. Mobile and removable devices will not be left unattended in public locations.

4. Upon request at any time, employees are responsible for returning all mobile and portable devices.

5. Devices requiring repair will be returned to the KHS Help Desk on a timely basis. Employees must never attempt to repair any device or authorize repairs by any third party.

6. Stolen or misplaced devices must be reported immediately to the KHS Help Desk. All passwords will immediately be changed to prevent unauthorized access.

7. SEI residing on a mobile device, cloud storage, and removable media, must be encrypted and password-protected

8. All SEI present on a mobile device, cloud storage, and removable media, is the property of KHS

9. Only approved cloud storage providers are authorized to store and transfer data. (Contact the KHS Help Desk for a list of authorized cloud storage providers.)

10. Transfer of SEI data to an individual and/or organization must be documented, submitted, and approved by completing a Data Exchange Request Form (DERF).

11. It is the employee's responsibility to adhere to all KHS policies and procedures regarding the appropriate access, use, storage, and disposal of SEI on mobile and removable devices.

M. De-Identification of PHI

1. Covered entities may use or disclose to a business associate PHI to create de-identified information. De-identified information is not considered PHI, and therefore, the use and disclosure requirements for PHI are not applicable to the de-identified information. De-identified information may not include any of the identifiers (*see section B above*) of the individual or of relatives, employers, or household members of the individual.

2. If a covered entity has actual knowledge that information could be used alone or in combination with other information to identify an individual who is a subject of the information, the information is not considered de-identified.

3. Covered entities may assign a code or other means of record identification to allow de-identified information to be re-identified provided that the code or other means of record identification:

a. Is not derived from or related to information about the individual and is not otherwise capable of being translated to identify the identity of the individual; and

b. Is not used or disclosed for any other purpose and does not disclose the mechanism for re-identification.

N. Minimum Necessary

1. KHS, including our subcontractors and contracted providers, will make reasonable efforts to limit access, use and disclosure of PHI to the minimum necessary information to accomplish the intended purpose of the request.

2. This "minimum necessary" standard does not apply to uses made pursuant to an appropriate authorization; uses that are required by law; or any other uses that are required for compliance with HIPAA.

3. KHS identifies those positions which require access to PHI to carry out their duties. Furthermore, for each position, KHS identifies the categories of PHI to which access is needed and any conditions appropriate to such access.

4. Any request for access to KHS member information that is out of the normal parameters for the job or procedure function of a KHS employee requires approval from the KHS Privacy Officer, or their designee.

5. This "minimum necessary" standard does not apply to disclosures to a health care provider for treatment; disclosures to the individual; disclosures made pursuant to an appropriate authorization; disclosures to the Secretary of the United States Department of Health and Human Services; disclosures that are required by the DHCS contract or law; or any other disclosures that are required for compliance with HIPAA.

O. Specially Protected PHI

1. Special protection is always afforded to psychotherapy notes. Use and/or disclosure of PHI related to psychotherapy notes must always have individual authorization except in the following circumstances:

   a. Use by the originator of the psychotherapy notes for treatment

   b. Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling

   c. Use to defend legal action or other proceeding brought against the covered entity by the individual

   d. Use or disclosure as required by law

e. Use or disclosure for health oversight activities of the originator of the psychotherapy notes

f. Disclosure to coroners or medical examiners

g. Use or disclosure as necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public

2. Special protection from unauthorized disclosure is afforded to other types of PHI. Disclosure of the following types of PHI must always have individual authorization:

a. Test results to detect the probable causative agent of acquired immune deficiency syndrome ("AIDS")

b. Alcohol, narcotic, and drug abuse patient records

c. Mental illness and developmental disabilities

d. Confidential communications falling within the scope of the physician patient or psychotherapist patient privilege.

e. Participation in outpatient treatment with a psychotherapist. This exception does not apply to the disclosure or use of information by a law enforcement agency or a regulatory agency when required for an investigation of unlawful activity or for licensing, certification, or regulatory purposes, unless the disclosure is otherwise prohibited by law.

f. Genetic test Results

3. Gender-Affirming Care

KHS, providers of health care, and/or any subcontractors will not release medical information related to a person or entity allowing a child to receive gender-affirming health care or gender-affirming mental health care in response to any civil action, including a foreign subpoena, based on another state's law that authorizes a person to bring a civil action against a person or entity that allows a child to receive gender-affirming health care or gender-affirming mental health care.

KHS, providers, and/or subcontractors will not release medical information to persons or entities who have requested that information and who are authorized by law to receive that information pursuant to Civil Code § 56.10(c), if the information is related to a person or entity allowing a child to receive gender-affirming health care or mental health care, and the information is being requested pursuant to another state's law that authorizes a person to bring a civil action against a person or entity who allows a child to receive gender-affirming health care or mental health care.

P. Personal Representatives

1. KHS, our subcontractors and providers must treat a personal representative as the individual. Personal representatives include the following:

    a. Persons with the authority to act on behalf of an adult or an emancipated minor in making decisions related to health care (for example, Power of Attorney; Legal Guardianship; etc.).

    b. Parents, guardians, or other persons acting *in locoparentis* with the authority to act on behalf of a minor in making decisions related to health care except that such a person may not be a personal representative, and the minor has authority to act as an individual in any of the following situations:

        i. The minor consents to such health care service; no other consent to such health care service is required by law; and the minor has not requested that such person be treated as the personal representative.

        ii. The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law contests to such health care service.

        iii. A parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

    c. Executors, administrators, or other persons who have the authority to act on behalf of a deceased individual or of the individual's estate

2. A covered entity may elect not to treat a person as the personal representative of an individual if:

    a. The covered entity has a reasonable belief that the individual has been or may be subjected to domestic violence, abuse, or neglect by such a person; or treating such person as the personal representative could endanger the individual; and

    b. The covered entity, in the exercise of professional judgement, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

Q. Permissible Use and Disclosure of Protected Health Information

1. PHI may be used without individual authorization for purposes of treatment, payment, health care operations, and as required by law[24]. No other use of PHI is permitted without explicit member authorization as described in the *Individual Authorization* section of this procedure.

a. For the covered entity's own treatment activities

b. For the treatment activities of a health care provider

c. To any entity contracting with KHS to monitor or administer care of enrollees for purposes of disease management programs and services, provided that the disease management services, and care are communicated to and/or authorized by a treating physician as required by California Civil Code §56.10(c)(17).

2. In cases where PHI is to be disclosed to an individual's relative, close friend, or any other person identified by the individual, the disclosure must be limited to that PHI which is directly relevant to such person's involvement with the individual's care. Prior to such disclosures, KHS, our subcontractors, and providers must do one of the following:

   a. Obtain the individual's agreement

   b. Provide the individual with the opportunity to object, and the individual does not express an objection

   c. Reasonably infer from the circumstances, based on the exercise of professional judgement, that the individual does not object to the disclosure

   d. If the individual is not present, or the opportunity to agree or object cannot practicably be provided because of the individual's incapacity or an emergency circumstance, determine whether the disclosure is in the best interest of the individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the individual's health care

3. Information contained in the health records shall be confidential and shall be disclosed only to authorized persons in accordance with federal, state and local laws.

4. KHS and our contracted subcontractors or providers may not require a patient, as a condition of receiving health care services, to sign an authorization, release, consent, or waiver that would permit the disclosure of medical information that otherwise may not be allowed under any provisions of law.

   a. Except to the extent expressly authorized by the patient or to the extent allowed by this policy, no contractor or corporation and its subsidiaries and affiliates shall further disclose medical information regarding a patient to any person or entity that is not engaged in providing direct health care services to the patient or his or her provider of health care or health care service plan or insurer or self-insured employer.

5. KHS will not use PHI in a manner inconsistent with this policy and our *Notice of Privacy Practices*. (See Attachment A).

a. PHI will only be used and disclosed in accordance with KHS policies and procedures.

b. Telecommuting or on-site, employees will not discuss confidential patient information with other employees unless there is a need to know (e.g., no lunchroom conversations of confidential patient information).

c. Employees will not discuss confidential patient information with unauthorized persons (e.g., friends, neighbors, relatives etc.).

d. KHS will not use data regarding race/ethnicity, language, gender identity or sexual orientation for decisions about coverage, benefits, and services.

6. KHS makes reasonable efforts to limit disclosure of PHI to the minimum necessary to accomplish the intended purpose of the disclosure, as described in section 10 above.

7. Prior to disclosure of PHI, staff should clearly determine all of the following:

   a. The request meets all necessary circumstances and limitations required for disclosure

   b. If authorization is required

   c. Verification of the authority of the requestor

   d. If accounting documentation is required

8. Prior to releasing PHI, the identity and authority of the requestor must be verified.

   a. To verify a member for incoming or outgoing calls, the caller must provide:

      i. Member's Full Name

      ii. CIN, KHS Member Identification number, or last four digits of their social security number

      iii. Date of Birth

   b. If someone other than the member is calling, the caller must provide their name, relationship, and the data elements above.

      i. If authorization is on file for the caller, PHI may be disclosed

      ii. If authorization is not on file for the caller, the member must be available to provide the above identifiers and verbal authorization to disclose PHI to the caller.

c. The identity of a public official may be verified by (1) presentation of an agency identification badge, other official credentials, or other proof of government status; (2) written requests on the appropriate government letterhead; or (3) if the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, MOU, or purchase order, that establishes that the person is acting on behalf of the public official. The authority of a public official may be verified by (1) a written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, on oral statement of such legal authority; or (2) a warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal.

d. Upon receipt of all required statements/documents, including a completed authorization if appropriate, the PHI is released subject to minimum necessary requirements and any applicable limitations.

e. For any disclosures requiring an accounting, staff must complete a *Disclosure of PHI – Accounting Form*.

f. The following documents are kept on file for a minimum of six years:

    i. Authorization for Use or Disclosure of Medical Information

    ii. Any required documents/statements, such as power of attorney or guardianship

    iii. *Disclosure of PHI – Accounting Form* and associated disclosure

9. The following subsections describe PHI disclosures that may be made without individual authorization. No other disclosure is permitted unless one of the following conditions is met: Explicit individual authorization is obtained; information is de-identified; information is converted to a limited data set subject to the data and recipient restrictions outlined in 45 CFR §164.514 (e).

    a. Treatment

    b. Payment

        i. For the covered entity's own payment activities

        ii. To another covered entity or a health care provider for the payment activities of the entity that receives the information

    c. Health Care Operations

        i. For the covered entity's own health care operations

i. To another covered entity for health care operations activities of the entity that received the information, if each entity either has or had a relationship with the individual who is the subject of the PHI being requested, the PHI pertains to such a relationship, and the disclosure is:

1. For a purpose listed in the definition of health care operations; or

2. For fraud and abuse detection or compliance

ii. A covered entity that participates in an organized health care arrangement may disclose PHI about an individual to another covered entity that participates in the organized health care arrangement for any health care operations activities of the organized health care arrangement.

iii. KHS may use data we collect for various reasons including but not limited to:

1. Identifying gaps in care and conducting outreach

2. quality assessments and improvement activities

3. population-based activities

4. Identify and reduce healthcare disparities

5. developing special programs

6. providing care coordination

7. developing member education and communications

8. evaluating KHS and provider performance

d. Notification of Involved Parties
Except for specially protected PHI, PHI may be disclosed without individual authorization for the purposes of notifying involved parties as follows:

i. To notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death

ii. To a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of the notifications described in this policy.

e. Public Health Activities

PHI may be disclosed for research purposes only if such research meets the requirements of 45 CFR §164.512(i). All disclosures to public health organizations are subject to accounting

requirements. PHI may be disclosed without individual authorization to public health organizations as follows:

i. A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority

ii. A public health authority or other appropriate government authority authorized by law to receive reports or child abuse or neglect

iii. A person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:

1. To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations.

2. To track FDA-regulated products.

3. To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback).

4. To conduct post marketing surveillance.

iv. A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation.

f. Activities Related to Decedents

Except for specially protected PHI, PHI may be disclosed without individual authorization for the following activities related to a decedent:

i. The County Coroner, when requested during an investigation by the coroner's office for the purpose of identifying the decedent or locating next of kin, or when

investigating deaths that may involve public health concerns, organ or tissue donation, child abuse, elder abuse, suicides, poisonings, accidents, sudden infant death, suspicious deaths, unknown deaths, or criminal deaths, or when otherwise authorized by the decedent's representative. Medical information requested by the coroner under this paragraph shall be limited to information regarding the patient who is the decedent and who is the subject of the investigation and shall be disclosed to the coroner without delay upon request. (Mandatory disclosure)

ii. To the County Coroner during an investigation. (Permissive disclosure)

iii. To an organ procurement organization or a tissue bank processing the tissue of a decedent for transplantation, but only with respect to the donor, for the purpose of aiding the transplant. (Permissive disclosure)

g. Reporting of Abuse, Neglect, and Domestic Violence
See *KHS Policy and Procedure #3.30-P – Domestic Violence/Criminal Act Reporting*

h. Judicial and Administrative Proceedings

Except for specially protected PHI, PHI may be disclosed without individual authorization during any judicial or administrative proceeding that meets either of the following requirements:

i. In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the PHI expressly authorized by such order.

ii. In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal if one of the following conditions is met:

1. The covered entity receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such part to ensure that the individual who is the subject of the PHI has been given notice of the request. This assurance must be in the form of a written statement and accompanying documentation demonstrating that (1) The requesting party has made a good faith attempt to provide written notice to the individual; (2) the notice included sufficient information about the litigation or proceeding to permit the individual to raise an objection to the court or administrative tribunal; and (3) the time for the individual to raise such objection has elapsed and either no objections were filed or all objections filed by the individual have been resolved and the disclosures being sought are consistent with such resolution.

2. The covered entity received satisfactory assurance from the party seeking the information that reasonable efforts have been made by

such party to secure a qualified protective order. This assurance must be in the form of a written statement and accompanying documentation demonstrating that (1) the parties to the dispute have agreed to a qualified protective order and have presented it to the court or administrative tribunal; or (2) the party seeking the PHI has requested a qualified protective order from such court or administrative tribunal. A qualified protective order is an order of a court or an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that (1) prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and (2) Requires the return to the covered entity or destruction of the PHI (including all copies made) at the end of the litigation or proceeding.

3. The covered entity, in lieu of receiving satisfactory assurance from the party seeking the PHI, performs the actions outlined in items 1 and 2 above.

i. Any such disclosure is limited to the extent that it is required by law, and it complies with and is limited to the relevant requirements of such law.

ii. Prior to releasing medical records that have been subpoenaed, KHS should be notified of the subpoena, and if appropriate, a copy of the medical records and subpoena should be sent to KHS.

iii. All disclosures to government authorities and/or law enforcement regarding judicial and administrative proceedings are subject to accounting requirements.

i. Law Enforcement Activities

Except for specially protected PHI, PHI may be disclosed without individual authorization for a law enforcement purpose to a law enforcement official in the following circumstances:

i. As required by law including laws that require the reporting of certain types of wounds or other physical injuries

ii. In compliance with and as limited by the relevant requirements of a court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer

iii. In compliance with and as limited by the relevant requirements of a grand jury subpoena

iv. In compliance with and as limited by the relevant requirements of an administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law if all of the following conditions are met:

1. The information sought is relevant and material to a legitimate law enforcement inquiry.

2. The request is specific and limited in scope to the extent reasonably practicable considering the purpose for which the information is sought.

3. De-identified information could not reasonably be used.

4. In response to a law enforcement official's request for PHI for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person. The covered entity may not disclose any PHI related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue. In such cases the covered entity may only disclose the following information:

    a. Name and address

    b. Date and place of birth

    c. Social security number

    d. ABO blood type and rh factor

    e. Type of injury

    f. Date and time of treatment

    g. Date and time of death

    h. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos

5. In response to a law enforcement official's request for PHI about an individual who is or is suspected to be a victim of a crime if the individual agrees to the disclosure, or the covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, if all of the following circumstances are met:

a. The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim

b. The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is unable to agree to the disclosure

c. The disclosure is in the best interests of the individual as determined by the covered entity in the exercise of professional judgement

j. To alert law enforcement of the death of an individual if the covered entity has suspicion that such death may have resulted from criminal conduct.

k. In response to criminal conduct that occurred on the covered entity's premises, if disclosure is limited to only that PHI which the covered entity believes in good faith constitutes evidence of such conduct

l. During the provision of emergency care, other than such emergency on the premises of the covered health care provider, for the purposes of alerting law enforcement of the commission and nature of a crime; the location of such crime or of the victim(s) of such crime; and the identity, description, and location of the perpetrator of such crime. This paragraph does not apply to emergencies resulting from abuse, neglect, or domestic violence of the individual in need of emergency health care.

m. In Response to Serious Threats to Health and Safety

Except for specially protected PHI, a covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose without authorization PHI regarding serious threats to health or safety in the following circumstances:

i. The covered entity, in good faith, believes the use or disclosure is (I) necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and (2) to a person(s) reasonably able to prevent or lessen the threat, including the target of the threat.

ii. The covered entity, in good faith, believes the use or disclosure is necessary for law enforcement authorities to identify or apprehend an individual (1) because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm

to the victim or (2) where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody. Such disclosure is not allowed if the information is learned during treatment to affect the propensity to commit the criminal conduct, counseling, therapy, or through a request by the individual for referral for such treatment, counseling, or therapy.

n. As Required by Law

PHI may be disclosed to the extent that such disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law. The disclosure must comply with any applicable restrictions and limitations.

o. To Employers

With the exception of specially protected PHI, PHI that is subject matter of workers' compensation proceedings may be disclosed without individual authorization to an employer concerning health care services to an employee provided at the request and expense of the employer if that information is relevant to a law suit or other claim or challenge involving the employer and employee, in which the patient has placed his/her medical history, physical or mental condition, or treatment in issue.

p. Business Associates

PHI may be disclosed without individual authorization as follows:

i. To a business associate that provides billing, claims management, medical data processing, or other administrative services for KHS, providers or for an insurer or other person responsible for paying for health care services rendered to the patient.

ii. To a business associate to create information that is not individually identifiable health information.

iii. PHI may be disclosed without individual authorization to a business associate only upon assurance that the business associate will appropriately safeguard the information. The business associate may also be allowed to create or receive PHI on KHS behalf upon such assurance. This assurance is obtained through either a business associate contract or a Memorandum of Understanding (MOU).

iv. Business associate contracts do not have to be received from entities performing enrollment/eligibility activities. MOUs, instead of business associate contracts, should be maintained with other governmental entities.

q. Business Associate Contracts/ MOUs

Contracts/MOUs may not authorize business associates to use or disclose PHI in a manner that violates this policy and procedure. Business associate contracts/MOUs must contain all of the following elements:

i. Establishment of the permitted and required uses and disclosures of PHI by the business associate.

ii. Permission for the use and disclosure of PHI for the proper management and administration of the business associate and for the carrying out of legal responsibilities of the business associate.

iii. Prohibition of the use or further disclosure of PHI other than as permitted or required by the contract or as required by law.

iv. Requirement to use of appropriate safeguards to prevent use or disclosure of PHI other than as provided for by the contract.

v. Requirement to report immediately to the covered entity upon discovery of any inappropriate use or disclosure of PHI in accordance with our contracts and Business Associate Agreements.

vi. Requirement that any agents, including a subcontractor, to whom PHI is provided must agree to the same restrictions and conditions that apply to the business associate.

vii. Requirement to make PHI available to the covered entity in such a manner that the covered entity may comply with an individual's request for disclosure, amendment, or accounting

viii. Requirement to incorporate any amendments requested by the individual into the business associate's record

ix. Requirement to make its internal practices, books, and records relating to the use and disclosure of PHI available to HHS for purposes of determining the covered entity's compliance with HIPAA

x. Requirement to, upon termination of the contract, return or destroy all PHI received from, or created, or received on behalf of the covered entity that the business associate 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 PHI and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible

xi. Authorization for termination of the contract by the covered entity if the covered entity determines that the business associate has violated a material term of the contract

xii. Upon knowledge of a pattern of activity or practice of a business associate that constitutes a material breach or violation of the business associate's obligation under the contract, the covered entity must take reasonable steps to cure the breach or end the violation, as applicable, and if such steps are unsuccessful will either terminate the contract or report the problem to the Secretary of the United States Department of Health and Human Services (HHS) if termination of the contract is not feasible.

r. Health Oversight Activities

Except for specially protected PHI, PHI may be disclosed without individual authorization for the following health oversight activities:

i. To any public or private entity responsible for licensing or accrediting the provider or health care service plan. However, no PHI may be removed from the premises except as expressly permitted or required by law.

ii. Covered entities may disclose PHI without individual authorization to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of any of the following:

1. The health care system.

2. Government benefit programs for which PHI is relevant to beneficiary eligibility.

3. Entities subject to government regulatory programs for which PHI is necessary for determining compliance with program standards.

4. Entities subject to civil rights laws for which PHI is necessary for determining compliance.

iii. Health oversight activities do not include an investigation or other activity in which the individual is the subject of the investigation or activity, and such investigation

or other activity does not arise out of and is not directly related to any of the following:

1. The receipt of health care

2. A claim for public benefits related to health

3. Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services

iv. Disclosures to government authorities regarding health oversight are not subject to accounting requirements as the oversight activities fall under the category "health care operations."

s. To the Member

KHS, our subcontractors, and providers may disclose PHI directly to the member and/or the member's authorized representative.

t. Other Rarely Occurring Situations

Federal regulations allow PHI to be disclosed in multiple circumstances that are not anticipated to apply to KHS or KHS providers. If these circumstances do occur, PHI should only be released as provided for in such federal regulations and the requirements for specialty protected health information should be applied.

i. For military and veterans' activities as described in 45 CFR §164.512(k)(l).

ii. For national security and intelligence activities as described in 45 CFR §164.512 (k)(2).

iii. For protective services for the President and others as described in 45 CFR §164.512(k)(3) .

iv. To correctional institutions and for other law enforcement custodial situations as described in 45 CPR §164.512 (k)(5).

v. For fundraising as described in 45 CPR §164.514 (f).

10. All disclosures to government authorities and/or law enforcement regarding law enforcement activities, or regarding serious threats to health or safety, are subject to accounting requirements.

11. In cases where PHI is to be disclosed to an individual's relative, close friend, or any other person identified by the individual, the disclosure must be limited to that PHI which is directly relevant to such person's involvement with payment or treatment related to the individual's health care. Prior to such disclosures, one of the following must occur and be documented:

    a. Obtain the individual's agreement

    b. Provide the individual with the opportunity to object, and the individual does not express an objection

    c. Reasonably infer from the circumstances, based on the exercise of professional judgement, that the individual does not object to the disclosure

    d. If the individual is not present, or the opportunity to agree or object cannot practicably be provided because of the individual's incapacity or an emergency circumstance, determine whether the disclosure is in the best interest of the individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the individual's health care

R. Individual's Access to PHI

1. KHS and our providers must provide PHI to the patient or the patient's representative for inspection within five (5) working days of receipt of a written request and upon payment of reasonable clerical costs incurred in locating and making the PHI available.

2. A patient who is a minor shall be entitled to inspect patient records pertaining only to health care of a type for which the minor is lawfully authorized to consent.

3. Inspection must be permitted during business hours and by the patient or the patient's representative who may be accompanied by one other person of his/her choosing.

4. Copies of PHI are provided within fifteen (15) calendar days of receipt of a written request for such copies and upon payment of a copying fee not to exceed 25 cents per page (50 cents per page copied from microfilm) and any additional reasonable clerical costs incurred in making the records available.

5. One copy will be provided at no charge upon proof that the records are needed to support an appeal regarding eligibility for a public benefit program. Such patients may be billed retroactively if the appeal is successful.

6. KHS provides the requested PHI in the form or format requested by the individual, if it is readily available in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by KHS and the individual.

7. If the entity receiving the request does not maintain the PHI that is subject to the individual's request but knows where the requested information is maintained, the covered entity will inform the individual where to direct the request for access.

8. Individuals may request, and KHS and other covered entities will accommodate, reasonable requests by individuals to receive communications of PHI from KHS by alternative means or at alternative locations.

9. For requests made to KHS, individuals must submit the request in writing to the following address:

    KHS Privacy Officer
    Compliance Department
    2900 Buck Owens Blvd.
    Bakersfield, CA 93308

10. Upon receipt of the written request, the Privacy Officer will work with the appropriate KHS staff to implement the request. The Privacy Officer will notify the individual of the disposition of the request.

11. The individual may inspect and/or pick up copies of the requested PHI at the KHS office. KHS will mail copies of the PHI to the individual upon request. KHS retains the right to charge individuals for the cost of copying and mailing requests

12. Denials of Access

    a. In general, an individual has a right of access to inspect and obtain a copy of his/her own PHI. The individual does not have the right of access to the following types of PHI:

        i. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

        ii. Information maintained by a covered entity that is subject to the Clinical Laboratory Improvements Amendments of 1988, 42 USC 263a to the extent the provision of access to the individual would be prohibited by law.

        iii. Information maintained by a covered entity that is exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).

    a. Covered entities may deny an individual access to the following types of PHI without providing the individual an opportunity for review:

i. Information to which the individual does not have a right of access as described in the preceding paragraph

ii. Information regarding an inmate of a correctional institution if obtaining such information would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.

iii. Information regarding research that includes treatment for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in such research, and the provider has informed the individual that the right of access will be reinstated upon completion of the research.

iv. Information contained in records that are subject to the Privacy Act, 5 USC §552a, if the denial of access under the Privacy Act would meet the requirements of that law.

v. Information obtained from someone other than a health care provider under a promise of confidentiality if the access requested would be reasonably likely to reveal the source of the information.

b. In certain situations, covered entities may also deny an individual access to PHI if the individual is given a right to have such denials reviewed. These situations include the following:

i. A licensed health care professional has determined, in the exercise of professional judgement, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person.

ii. The PHI refers to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgement, that the access requested is reasonably likely to cause substantial harm to such other person.

iii. The request for access is made by the individual's personal representative and a licensed health care professional has determined in the exercise of professional judgement, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

c. If access is denied for the reasons above, the individual has the right to have the denial

reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. Access must be provided or denied based on the decision of such health care professional.

d. Denials must be communicated to the individual in writing and include the following:

i. The basis for the denial.

ii. If applicable, a statement of the individual's review rights, including a description of how the individual may access such rights.

iii. A description of how the individual may complain to KHS (including name/title and telephone number of the contact person) or the Secretary of the United States Department of Health and Human Services (HHS).

S. Accounting of Disclosures

1. The KHS Privacy Official is responsible for receiving and processing accounting of disclosure requests.

2. Providers must have a written process for responding to an individual's request for an accounting of disclosures. This documentation must include the titles of the persons or offices responsible for receiving and processing such requests.

3. An individual has the right to receive an accounting of disclosures of PHI made in the six years prior to the date on which the accounting is requested, except for disclosures:

a. To conduct treatment, payment, and health care operations

b. To individuals about their own PHI

c. Pursuant to an authorization

d. For the facility's directory or to persons involved in the individuals care or other notification purposes as provided in 45 CFR §164.510

e. For national security and intelligence activities as described in 45 CFR §164.512(k)(2)

f. To correctional institutions and for other law enforcement custodial situations as described in 45 CFR §164.512 (k)(5)

g. That are part of a limited data set subject to the data and recipient restrictions outlined in 45 CFR §164.514 (e)

h. Made prior to April 14, 2003

4. In certain circumstances, a health oversight agency or law enforcement official may request that an individual's right to receive an accounting of disclosures to such agency/official be temporarily suspended. Such requests are forwarded to the Privacy Official. The Privacy Official manages such requests in accordance with 45 CFR §164.528 (a)(2).

5. The accounting is provided in writing within sixty (60) days of the request and includes the following for each disclosure:

    a. The date of the disclosure

    b. The name (and address if known) of the recipient

    c. A brief description of the information

    d. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure

T. Individual Authorization

A valid patient authorization must be received prior to releasing confidential information or medical records that do not meet the requirements for disclosure without individual authorization.

The California Confidentiality of Medical Information Act permits health plans, like KHS, to receive and release medical information about its members without their written consent as necessary to administer the health plan (California Civil Code Section 56.10(c)).

1. Any individual authorization must be kept in the patient's medical records file for a minimum of six years from the date of creation or the last date the authorization was in effect, whichever is later.

2. A copy of the signed authorization must be provided to the individual.

3. The KHS authorization form is included as Attachment B.

4. A recipient of medical information pursuant to an authorization may not further disclose that information except in accordance with a new valid authorization or as specifically required or permitted by law.

5. No provider of health care, health care service plan, or contractor may require a patient, as a condition of receiving health care services, to sign an authorization, release, consent, or waiver that would permit the disclosure of medical information that otherwise might not be disclosed under law.

6. For an authorization for a provider, health care service plan, or contractor to release information to be valid, it must contain the following elements:

    a. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion

    b. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure

    c. The name or other specific identification of the person(s), or class of persons, to whom the provider may make the requested disclosure

    d. A description of each purpose of the requested use or disclosure including the specific uses and limitations on the use of medical information by the authorized recipient

    e. State a specific date after which the provider is no longer authorized to disclose the medical information

    f. Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such person's authority to act for the individual must also be provided

    g. A statement notifying the individual of his/her right to revoke the authorization in writing including any exceptions to the right to revoke and a description of how the individual may revoke the authorization

    h. A statement that the provider may not condition treatment or payment on receipt of the authorization

    i. A statement notifying the individual of the potential for information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient and no longer be protected by HIPAA.

    j. A statement that the person signing the authorization has a right to receive a copy of it.

    k. Handwritten by the person who signs it or typewritten in at least 8-point font

    l. Clearly separate from any other language present on the same page

    m. In plain language

    n. Executed by a signature that serves no purpose other than to execute the authorization

7. An authorization is not valid if the document submitted has any of the following defects:

    a. The expiration date has passed

b. The required elements section of the authorization has not been filled out completely

c. The authorization is known by the covered entity to have been revoked

d. Any material information in the authorization is known by the covered entity to be false

8. Additional Requirements for Information Relating to Outpatient Psychotherapy. In addition to the elements described in the previous section, an authorization for information related to outpatient psychotherapy must include the following:

   a. Signature of the requestor

   b. Length of time during which the information will be kept before being destroyed or disposed of

   c. Statement that the information will not be used for other purposes and will be destroyed within the designated time frame.

   d. The time frame may be extended, provided that the entity that supplied the information is notified of the extension, the reasons for the extension, the intended uses, and the expected date the information will be destroyed.

   e. The person or entity requesting the information submits a copy of the written request to the patient within thirty (30) days of receipt of the information requested unless the patient has signed a written waiver.

9. Cancellation or Modification of an Authorization

   a. Upon receipt of a written notice from a potential signer of an authorization, the holder must modify or cancel the authorization in accordance with the potential signer's written instruction

U. Enforcement

1. KHS is committed to the confidentiality and security of patient information. Any person found in violation of this Policy and Procedure will be subject to disciplinary action up to and including termination and may be prosecuted according to Federal and/or State law. Any such disciplinary action is documented and maintained for a minimum of six years.

2. Any person who knowingly releases or possesses confidential information concerning persons who have applied for or who have been granted any form of Medi-Cal benefits or benefits under Chapter 8 (commencing with Section 14200) or Chapter 8.7 (commencing with Section 14520) for which state or federal funds are made available in violation of this section is guilty of a misdemeanor.

3. Covered entities must have and apply appropriate sanctions against members of its workforce who fail to comply with privacy policies and procedures. Applied sanctions must be documented.

V. Unauthorized Use or Disclosure

1. Upon discovery of unauthorized disclosure of member PHI or PI, KHS shall immediately report and investigate the incident and make efforts to mitigate harm to the affected individual(s) as required by the DHCS Contract, and pursuant to HIPAA laws.

    a. A breach is considered discovered on the first day on which the breach is known, or would have been known, to any person who is an employee, officer, or agent of KHS. Incidents are to be reported to the KHS Compliance Department immediately upon discovery. The Compliance Department is responsible for reviewing, logging, and reporting all incidents.

    b. Compliance will immediately notify the DHCS by telephone plus e-mail or fax upon the discovery of a breach of unsecured PHI or PI in electronic media or in any other media if the PHI or PI was or is reasonably believed to have been accessed or acquired by an unauthorized person.

    c. Compliance will notify the DHCS within 24 hours by email or fax of the discovery of any suspected security incident, intrusion, or unauthorized access, use or disclosure of PHI or PI in violation of the DHCS Contract, or potential loss of confidential data affecting the DHCS Contract.

2. A complete PIR of the investigation will be provided to DHCS within ten (10) working days of discovery of the breach or unauthorized use or disclosure. The report shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of state and federal law; a full detailed corrective action plan including measures taken to mitigate harm to the affected member(s).

3. DHCS will review and approve the documentation submitted and make the determination of whether a breach occurred. If individual notifications are required, DHCS shall review and approve the notice prior to KHS sending the notice to the affected members.

4. Notification by a Business Associate

    a. If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify KHS following the discovery of the breach.

    b. A business associate must provide notice to KHS without unreasonable delay and no later than sixty (60) days from the discovery of the breach. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any information required to be provided by the covered entity in its notification to affected individuals.

5. Breach Notification to Members

    a. KHS, our subcontractors, and our providers that maintain computerized data which includes an individual's name and any of the following items must notify a California resident when that individual's information was or is reasonably believed to have been acquired by an unauthorized person due to a breach of the security of the data:

        i. Social Security Number

        ii. Driver's license number or California Identification Card Number

        iii. An account, credit, or debit card number in combination with a required security code, access code, or password that would permit access to an individual's financial account

    b. Notice may be provided by either of the following methods:

        i. Written notice

        ii. Electronic notice if the notice provided is consistent with the provisions regarding electronic records and signatures set for in §7001 of Title 15 of the United States Code

    c. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

    d. Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information.

    e. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically.

    f. If the covered entity has insufficient or out-of-date contact information for ten (10) or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside.

    g. If the covered entity has insufficient or out-of-date contact information for fewer than ten (10) individuals, the covered entity may provide substitute notice by an alternative form of written, telephone, or other means.

h. These individual notifications must be provided without unreasonable delay and in no case later than sixty (60) days following the discovery of a breach and must include, to the extent possible:

i. Description of the breach,

ii. Description of the types of information that were involved in the breach

iii. The steps affected individuals should take to protect themselves from potential harm

iv. A brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches

v. Contact information for the covered entity.

vi. For substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the covered entity to determine if their protected health information was involved in the breach.

W. Breaches of Security

1. KHS will notify the Department of Health Care Services within 24 hours by email or fax of the discovery of any suspected security incident, intrusion, or unauthorized access, use or disclosure of PHI or PI in violation of the DHCS Contract, or potential loss of confidential data affecting the DHCS Contract.

2. A complete PIR of the investigation will be provided to DHCS within ten (10) working days of discovery of the breach or unauthorized use or disclosure. The report shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of state and federal law; a full detailed corrective action plan including measures taken to mitigate harm to the affected member(s).

3. For breaches that affect fewer than 500 individuals, a covered entity must provide the Secretary with notice annually.

4. All notifications of breaches occurring in a calendar year must be submitted within sixty (60) days of the end of the calendar year in which the breaches occurred. This notice must be submitted electronically by following the link below and completing all information required on the breach notification form. A separate form must be completed for every breach that has occurred during the calendar year.

http://ocmotifications.hhs.gov/

5. If a covered entity that has submitted a breach notification form to the Secretary discovers additional information to report, the covered entity may submit an additional form, checking the appropriate box to signal that it is an updated submission. If, at the time of submission of the form, it is unclear how many individuals are affected by a breach, an estimated number of individuals affected will be provided. As this information becomes available, an additional breach report will be submitted as an addendum to the initial report.

6. If a breach affects 500 or more individuals, a covered entity must provide the Secretary with notice of the breach without unreasonable delay and in no case later than sixty (60) days from discovery of the breach. This notice must be submitted electronically by following the link below and completing all information required on the breach notification form.

http://ocmotifications.hhs.gov/

7. If a covered entity that has submitted a breach notification form to the Secretary discovers additional information to report, the covered entity may submit an additional form, checking the appropriate box to signal that it is an updated submission. If, at the time of submission of the form, it is unclear how many individuals are affected by a breach, an estimated number of individuals affected will be provided. As this information becomes available, an additional breach report may be submitted as an addendum to the initial report

8. Media Notice - Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than sixty (60) days following the discovery of a breach and must include the same information required for the individual notice.

9. Burden of Proof - Covered entities and business associates have the burden of proof to demonstrate that all required notifications have been provided or that a use or disclosure of unsecured protected health information did not constitute a breach.

10. This section also requires covered entities to comply with several other provisions of the Privacy Rule with respect to breach notification. For example, covered entities must:

    a. Have written policies and procedures regarding breach notification

    b. Train employees on these policies and procedures
    c. Develop and apply appropriate sanctions against employees who do not comply with these policies and procedures.

X. Compliance Reviews

1. All compliance review activities will be coordinated by the Compliance Department under the supervision of the Chief Compliance and Fraud Prevention Officer.

2. The United States Department of Health and Human Services (HHS) may conduct compliance reviews to determine compliance with HIPAA regulations.

3. KHS retains records and submits compliance reports as required by HHS.

4. KHS cooperates with HHS in any complaint investigations or compliance reviews. This cooperation includes permitting access during normal business hours to facilities, books, records, accounts, and other sources of information, including PHI, that are pertinent to ascertaining compliance.

Y. Reports of Suspected Violations by Employees

Employees have a responsibility to report suspected violations of any statute, regulation, or guideline applicable to government funded health care programs or KHS policies and procedures. Employees are informed that they have the right to use the KHS Confidential Disclosure Program (Ethics Line) to report complaints of suspected violations of KHS confidentiality policies, corporate integrity issues, and/or any other area of concern.

Reports of suspected violations may be reported to the Ethics Line or the Privacy Official. No retribution or retaliatory action will be taken against an employee for having filed a complaint.

Z. Training

1. KHS:

   KHS employees are provided training within thirty (30) days of employment. Employees whose functions are affected by a material change to privacy policies and procedures are provided training on the revised policy and procedures within thirty (30) days of the effective date of the change. All training activities are documented and maintained by the Department Head for no less than six years.

   At the time of hire employees are required to sign a *Confidentiality of Information statement* at orientation and given a copy of same.

2. Subcontractors, Downstream Subcontractors and Network Providers:

   KHS providers and delegated entities must also train all members of its workforce on policies and procedures regarding PHI as necessary and appropriate for them to conduct their function within the covered entity. Such training must be provided according to the following schedule, documented, and maintained on file for no less than six years:

   a. To each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce

   b. To each member of the covered entity's workforce whose functions are affected by a

material change in the policies or procedures regarding PHI within a reasonable period of the effective date of the change

AA. Member Notification

1. KHS maintains a Notice of Privacy Practices (NPP) that meets the format and content requirements of 45 CFR §164.520 and explains how KHS maintains the confidentiality of medical information in accordance with California Health and Safety Code 1364.5 (See Attachment A).

2. KHS provides all members with a copy of the appropriate *NPP* via the *Member Handbook* upon enrollment.

3. KHS also provides a copy of the *NPP*, which includes information on how KHS maintains the confidentiality of medical information, to any person upon request.

4. KHS promptly revises and distributes the *Notice of Privacy Practices* whenever there is a material change to the uses or disclosures, the individual's rights, KHS' legal duties, or other privacy practices stated in the notice. Except when required by law, such changes may not be implemented prior to the effective date and distribution of the notice.

5. In all cases, the revised notice will be distributed within sixty (60) days of revision to individuals then covered by a KHS plan.

6. The Privacy Official will provide further information about matters covered by the NPP, including confidentiality of medical information.

7. KHS providers must maintain a *Notice of Privacy Practices (NPP)* that meets the format and content requirements of 45 CFR §164.520.
   a. A covered health care provider that has a direct treatment relationship with an individual must provide the notice no later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider; or as soon as reasonably practical in an emergency treatment situation.

   b. Covered providers must make a good faith effort to obtain written acknowledgement of receipt of the notice. If such acknowledgement cannot be obtained, the covered provider must document the good faith efforts to do so and reason for the failure.

   c. The NPP must be available on site and posted in a clear and prominent location. Whenever the NPP is revised, it must be made available upon request.

d. A covered provider must promptly revise and distribute the *NPP* whenever there is a material change to the uses or disclosures, the individual's rights, the provider's legal duties, or other privacy practices stated in the notice. Except when required by law, such changes may not be implemented prior to the effective date and distribution of the notice.

e. A contact person must be appointed who is able to provide further information about matters covered by the *NPP*.

BB. Confidentiality of Medical Information

1. Sensitive Services:

   a. KHS will not disclose medical information related to sensitive health care services provided to a protected individual to the primary subscriber or any plan enrollees other than the protected individual receiving care, absent an express authorization of the protected individual.

   b. KHS will not require a protected individual to obtain the primary subscriber's other enrollee authorization to receive sensitive services or to submit a claim for sensitive services if the protected individual has the right to consent to care.

   c. KHS employees, providers, and delegated entities must adhere to the steps outlined in *Policy 3.20, Sensitive Services.*

2. Confidential Communications:

   a. KHS will notify subscribers and enrollees they may request a confidential communication, how to make the request, and provide this information at the time of initial enrollment and annually thereafter.

3. Communications (written, verbal or electronic communications) regarding a protected individual's receipt of sensitive services shall include:

   a. Bills and attempts to collect payment.

   b. A notice of adverse benefits determinations.

   c. An explanation of benefits notice.

      i. A plan's request for additional information regarding a claim.

      ii. A notice of a contested claim.

iii. The name and address of a provider, description of services provided, and other information related to a visit.

iv. Any written, oral, or electronic communication from a plan that contains protected health information.

4. KHS will permit and accommodate requests from subscribers or enrollees for confidential communication in the form and format requested, if readily producible in the requested form and format, or at alternative locations.

5. Requests for Confidential Communications may be made if the member clearly states either that the communication discloses medical information or provides name and address relating to receipt of sensitive services, or that disclosure of all or part of the medical information or provider name and address could endanger the member. KHS will not require an explanation as to the basis for a subscriber's or enrollee's statement that disclosure could endanger the subscriber or enrollee.

6. Members may request Confidential Communications by calling member services or sending a request in writing:

KHS Privacy Officer
Compliance Department
2900 Buck Owens Blvd.
Bakersfield, CA 93308

7. Confidential communication requests will be valid until the subscriber or enrollee submits a revocation of the request or a new confidential communication request is submitted.

8. Processing Requests for Confidential Communications:

   a. KHS's Member Service Department may assist the Member, or the Member's Personal Representative, in completing the Confidential Communications Request. A Confidential Communications Form will be provided upon request, but the member is not required to use the KHS form, as long as the appropriate information is provided with the member's request.

   b. All requests for Confidential Communications will be routed to the Compliance Department within one business day of receipt.

   c. The KHS Privacy Officer, or designee, will:

      i. Acknowledge receipt, and review and implement confidential communications requests within seven (7) calendar days of receipt of an electronic or telephonic request or within fourteen (14) calendar days of receipt by first-class mail.

      ii. Requests will be approved when the member clearly states either that the communication discloses medical information or provider name and address relating

to receipt of sensitive services or that disclosure of all or part of the medical information or provider name and address could endanger the member by receiving the KHS information at the address, phone number, or email address on file.

iii. Enter a member alert in the system, which will ensure protected individuals receiving sensitive services, and members with confidential communication requests, are sent to the designated alternative mailing address, email address, or telephone number.

iv. If the protected individual has not designated an alternative mailing address, email address, or telephone number, the health insurer shall send or make all communications related to the protected individual's receipt of sensitive services in the name of the protected individual at the address or telephone number on file.

d. The confidential communication request shall apply to all communications that disclose medical information or provider name and address related to receipt of medical services by the individual requesting the confidential communication.

CC. Member Complaints

1. Covered entities must designate a contact person or office who is responsible for receiving complaints related to PHI. Providers should forward all such complaints from KHS Plan members to the KHS Grievance Coordinator.

2. Complaints regarding PHI are subject to the policies and procedures outlined in *KHS Policy and Procedure #5.01 - Grievance Process.*

DD. Delegation Oversight

1. KHS, contracted providers, subcontractors and downstream subcontractors take steps as required by Assembly Bill 1184 to protect the confidentiality of medical information as required.

2. KHS, contracted providers, subcontractors, and downstream subcontractors do not condition enrollment or coverage on the waiver of the confidentiality rights provided in Civil Code section 56.107.

3. KHS is responsible for ensuring that their network providers, subcontractors, and downstream subcontractors comply with all applicable state and federal laws and regulations, contract requirements, and other DHCS and DMHC guidance, including APLs and Policy Letters.

4. KHS will communicate the policy requirements to all network providers, subcontractors, and downstream subcontractors.

5. KHS will ensure that all our own policies and procedures, as well as the policies, procedures, and practices of any delegates or subcontractors comply with these requirements and those located in any applicable APL.

V. ATTACHMENTS

Attachment A: Notice of Privacy Practices
Attachment B: Authorized Representative Form
Attachment C: Confidential Communication Request Form
Attachment D: Disclosure of PHI Accounting Form

VI. REFERENCES

Reference Type	Specific Reference
DHCS Contract (Specify Section)	Exhibit G
All Plan Letter(s) (APL)	DMHC APL 22-010
All Plan Letter(s)	DMHC APL 22-031
Regulatory	HIPAA eCFR :: 45 CFR Part 160 eCFR :: 45 CFR Part 164
Regulatory	CCR Title 22 §75055(b)
Regulatory	California Confidentiality of Medical Information Act California Civil Code, division 1, part 2.6 – Confidentiality of Medical Information
Regulatory	California Health & Safety Code § 123110
Regulatory	HITECH Act eCFR :: 45 CFR Part 170
Regulatory	California Civil Code §1798.82
Internal	KHS Code of Conduct
Internal	KHS Compliance Program
Internal	KHS Compliance Guide
14.61	Delegation
Internal	Employee Handbook

VII. REVISION HISTORY

Action	Date	Brief Description of Updates	Author
Revised	04/2024	Updated further for NCQA elements HE 2-F/HE 2-G to include additional IT components.	Director of Compliance Director Technical Operations & Security
Revised	12/2023	Updated for NCQA elements HE 2-F and HE 2-G regarding use and disclosure of race/ethnicity, language, gender identity and sexual orientation data; created public version for posting to website	Director of Compliance
Revised	10/2023	Updated Attachment A, Notice of Privacy Practices, to coincide with 2024 EOC; DMHC Approved 10/23/2023. DHCS Approved 10/23/2023	Director of Compliance
Revised	05/2023	Updated for 2024 DHCS Contract R.0159; DHCS approved 06/07/2023.	Director of Compliance
Revised	04/2023	Updated to include portions of 2.27 & 2.28 and elements from DMHC APL 22-010. AB1184; Confidentiality of Medical Information. The DMHC approved the policy on 2/1/2023, filing No. 20222271	Director of Compliance
Revised	02/2023	Updated to include information regarding DMHC APL 22-031 and SB 107. DMHC Approved 02/01/2023.	Director of Compliance
Revised	04/2022	Updated to include portions of 2.27 & 2.28 and elements from DMHC APL 22-010	Director of Compliance
Revised	08/2020	Updated to include telecommuting or on-worksite language, address update. Revision 2012-08 Breaches of Security section deleted referenced policy 2.28-P as to not duplicate information. Training documents are to be maintained for no less than six years. Revised information on training of employees. Policy renumbered to 14.03-I to fit under AIS/Compliance Department responsibility.	Compliance
Revised	06/2007	Revised per DHS/DMHC Medical Audit comments 5/13/2007. Language added to comply with MMCD Letters 06001 and	Compliance

		06005	
Revised	03/2007	Revised per DHS/DMHC Medical Audit Review Category 4.4.1 (YE 10/30/2006).	YE
Revised	10/2003	Revised to comply with HIPAA and AB700 (2002). Formerly titled "Employee Confidentiality". Employee confidentiality of business information is addressed in the Personnel Manual.	Compliance
Revised	06/2001	Revised to comply with changes to the Confidentiality of Medical Information Act. Submission to DMHC required by 06/30/01.	Compliance
		Formerly: 1.10 Changed to #100.10 during revision of internal/external numbering system.	Compliance
Effective	08/1997	Initial Policy	Compliance

VIII. APPROVALS

Committees | Board (if applicable)	**Date Reviewed**	**Date Approved**
Choose an item.		

Regulatory Agencies (if applicable)	**Date Reviewed**	**Date Approved**
Department of Managed Health Care (DMHC)	3/30/2024, APL 23-025 eFiling 20241627	5/14/2024
Department of Health Care Services (DHCS)	Notice of Privacy Practices (Attachment A)	10/23/2023
Department of Managed Health Care (DMHC)	Notice of Privacy Practices (Attachment A)	10/23/2023
Department of Health Care Services (DHCS)	5/22/2023, 2024 OR (R.0159)	6/7/2023
Department of Managed Health Care (DMHC)	efiling # 20222271-1	2/1/2023
Department of Managed Health Care (DMHC)	1/11/2023, APL 22-031	2/1/2023

Chief Executive Leadership Approval *		
Title	**Signature**	**Date Approved**
Chief Executive Officer		
Chief Medical Officer		
Chief Operating Officer		
Chief Financial Officer		
Chief Compliance and Fraud Prevention Officer		
Chief Health Equity Officer		
Chief Legal and Human Resources Officer		
Deputy Chief Information Officer		
*Signatures are kept on file for reference but will not be on the published copy		

KERN HEALTH SYSTEMS

Policy and Procedure Review

KHS Policy & Procedure: 14.03-P Protected Health Information

Last approved version: N/A

Reason for revision: Reformatted; included additional requirements from various APLs and policy versions

Director Approval		
Title	**Signature**	**Date Approved**
N/A		

Date posted to public drive: _____

Date posted to website ("P" policies only) : _____