KERN HEALTH SYSTEMS

KERN HEALTH SYSTEMS POLICY AND PROCEDURES					
SUBJECT: Medical Records and Other Protected Health Information – Content, Maintenance, and Security				POLICY #: 2.27-P	
DEPARTMENT: Quality Improvement Department					
Effective Date: 08/1997	Review/Revised Date: 06/06/2016	DMHC		PAC COMMITTEE	
		DHCS	X	QI/UM COMMITTEE	
		BOD		FINANCE COMMITTEE	

Douglas A. Hayward
Chief Executive Officer — Date 6/6/16

Chief Medical Officer — Date 6/6/2016

Chief Operating Officer — Date 6/6/16

Director of Compliance and Regulatory Affairs — Date 6-2-16

Director of Marketing and Member Services — Date 5/26/16

Deborah L. Lauer RN
Administrative Director of Health Services — Date 5/26/16

POLICY:
Confidential patient information shall be created, 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 an unauthorized person or entity.[1]

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) (Code of Federal Regulations Title 45 Parts 160 and 164).

Contractor shall ensure that appropriate Medical Records for Members, pursuant to Title 28, CCR, Section 1300.80(b)(4) and 42 USC S 139a(w), are available to health care providers at each encounter in accordance with Title 28, CCR, Section 1300.67.1(c) and Title 22, CCR, Section 53861 and MMCD Policy Letter 02-02.

DEFINITIONS:

See *KHS Policy and Procedure #2.28-P Medical Records and Other Protected Health Information – Privacy, Use, and Disclosure*.

PROCEDURES:

1.0 PROVIDER POLICIES AND PROCEDURES

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 release of information and obtaining consent for treatment.

D. Policies and procedures to maintain medical records in a legible, current, detailed, organized and comprehensive manner. Records may be electronic or hard copy.

E. Documentation of the titles of persons responsible for receiving and processing requests for amendments by individuals [2]

F. A process/system established on site provides for the availability of medical records, including outpatient, inpatient, referral services, and significant telephone consultations for patient encounters. Medical records are readily retrievable for scheduled patient's encounters. Medical documents are filed in a timely manner to ensure availability for patient encounters. Medical records are filed that allows for ease of accessibility within the facility, or in an approved health record storage facility off the facility premises (22 CCR, S75055).

2.0 INFORMATION REQUIRED TO BE IN THE MEDICAL RECORD

A complete medical record must be maintained for each family member in accordance with Title 22, CCR, Section 53861 and/or DHCS PL 14-004 and reflect all aspects of patient care, including ancillary services. At a minimum it must include:

A. Member name and date of birth on each page. Personal/biographical data must include the patient's complete name, address, home and work telephone number, name of nearest relative, emergency contact, driver's license number, social security number, employer, marital status and name of parent(s) if patient is a minor.

B. Member's preferred language (if other than English) prominently noted in the record, as well as the request or refusal of language/interpretation services. Friends or family members should not be used as interpreters, unless specifically requested by the member. The member's refusal of language/interpretations services is documented.

C. All entries dated and author identified, using the first initial, last name and title of the person making the entry, regardless of his/her position in the office. The entries must include at a minimum, the subjective complaints, the objective findings, and the plan for diagnosis and treatment.

D. A problem list identifying significant past surgical procedures and past and current diagnoses or problems.

E. Current continuous medications are listed. List of current, on-going medications identifies the medication name, strength, dosage, route, and start/stop dates. Discontinued medications are noted on the medication list or in progress notes.

F. A complete record of immunizations and health maintenance or preventive services rendered.

G. Allergies and adverse reactions prominently noted. If a member has no allergies or adverse reactions, "No Known Allergies" (NKA), "No Known Drug Allergies" (NKDA), or 0 is documented.

H. All informed consent documentation, including the human sterilization consent procedures.

I. Reports of emergency care provided (directly by the contracted provider or through an emergency room) and the hospital discharge summaries for all hospital admissions.

J. All consultations, referrals and specialists reports, and all pathology and laboratory reports. Any abnormal results must have an explicit notation in the record stating the follow-up initiated.

K. For medical records of adults, documentation of whether the individual has been informed and has executed and advanced directive such as a Durable Power of Attorney for Health Care.

L. Health education behavioral assessment and referrals to health education services.

M. The assigned PCP is *always* identified when there is more than one PCP on site and/or when the patient has selected health care from a non-physician medical practitioner.

N. Missed appointments and follow-up contracts/outreach efforts are noted. Documentation includes incidents of missed/broken appointments (cancellations of "no Shows") for PCP examinations, diagnostic procedures, lab tests, specialty appointments, and/or other referral services. Attempts to contact the patient and/or parent guardian (if minor), and the results of follow-up actions are also documented. Documentation of No Show appointments and cancellation as per *KHS Policy #2.01-P General Exam Guidelines.*

O. Contents and format of printed and/or electronic records within the practice site are uniformly organized. Contents are securely fastened, attached or bound to prevent medical record loss. Electronic medical record information is readily available.

P. All entries are signed, dated and legible. Signature includes the first initial, last name and title. Initials may be used if signatures are specifically identified elsewhere in the medical record (e.g. signature page). Date includes month/day/year. Entries are in reasonable consecutive order by date. Handwritten documentation, signatures and initials are entered in ink that can be readily copied. Handwritten documentation does not contain skipped lines or empty spaces where information can be added. Entries are not backdated or inserted into spaces above previous entries. Omissions are charted as a new entry. Late entries are explained in the medical record, signed and dated.

Q. Errors are corrected according to legal medical documentation standards. The person that makes the documentation error corrects the error. A single line is drawn through the error, with "error" written above or near the lined-through incorrect entry. The corrected information is written as a separate entry and includes date of the entry, signature (or initials), and title. There are no unexplained cross-outs, erased entries or use of correction fluid. Both the original entry and corrected entry are clearly

preserved.

3.0 INDIVIDUAL'S RIGHT TO PROVIDE A WRITTEN ADDENDUM TO PROTECTED HEALTH INFORMATION[3]

An individual has the right to have a covered entity amend PHI. A covered entity may deny an individual's request for amendment if it determines that the PHI

A. Was not created by the covered entity, 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.
B. Qualifies as PHI to which the individual can be denied access to inspection
C. Is accurate and complete

The covered entity must act on the individual's request for an amendment no later than 60 days after such a request.

3.1 Accepted Amendments

The covered entity must 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. 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:

A. Persons identified by the individual as having received PHI about the individual and needing the amendment,
B. 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.

3.2 Denied Amendments

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

A. The basis for the denial
B. The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement
C. 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
D. 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.

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.

All related amendment documentation must be included with all future disclosures of the related PHI.

4.0 DISPOSAL OF PROTECTED HEALTH INFORMATION

KHS contracted 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 in any individually identifiable form by any other person or entity.[4] Disposal or destruction should be complete and thorough. Any material containing confidential information should be thoroughly shredded prior to disposal in waste paper baskets and other means of disposal. This applies to forms, letters, and other such items.

Medical records must be kept for a minimum of 7 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 seven years.[5]

5.0 PROVIDER EDUCATION AND MONITORING

This policy and procedure is included in the Provider Administrative Manual.

Compliance with this policy and procedure is monitored by the Quality Improvement (QI) Department through the facility site review process. For additional information on this process see *KHS Policy and Procedure #2.22-P Facility Site Review.* Additional reviews of a specific provider's medical records may be performed as deemed necessary by the Chief Executive Officer, Chief Medical Officer, or Administrative Director of Health Services.

6.0 SECURITY OF PROTECTED HEALTH INFORMATION

KHS contracted providers who create, maintain, preserve, or store medical information must do so in a manner that preserves the confidentiality of the information and does not allow for retrieval in any individually identifiable form by any other person or entity.[6] An individual must be assigned the responsibility of securing and maintaining medical records at each network provider office.

Providers that utilize electronic recordkeeping systems only, must comply with the additional requirements of California Health and Safety Code §123149 as appropriate.

6.1 De-identification of PHI[7]

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 following identifiers of the individual or of relatives, employers, or household members of the individual:

A. Names

B. 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:

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

2. The initial 3 digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

C. 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;
D. Telephone numbers
E. Fax numbers
F. Electronic mail addresses
G. Social security numbers
H. Medical record numbers
I. Health plan beneficiary numbers
J. Account numbers
K. Certificate/license numbers
L. Vehicle identifiers and serial numbers, including license plate numbers
M. Device identifiers and serial numbers
N. Web Universal Resource Locators (URLs)
O. Internet Protocol (IP) address numbers
P. Biometric identifiers, including finger and voice prints
Q. Full face photographic images and any comparable images
R. Any other unique identifying number, characteristic, or code

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.

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 so as 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.

6.2 Notification by a Business Associate

If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than 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.

6.3 Breaches of Security – Notice to Individuals[8]

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:

A. Social Security Number
B. Driver's license number or California Identification Card Number
C. An account, credit or debit card number in combination with an required security code, access code, or password that would permit access to an individual's financial account

Notice may be provided by either of the following methods:

A. Written notice
B. 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

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.

6.4 Individual Notice

Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information. 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. If the covered entity has insufficient or out-of-date contact information for 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. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written, telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity. Additionally, 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.

6.5 Breaches of Security

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.

An updated DHCS PIR of the investigation will be provided to DHCS within seventy-two (72) hours of the discovery by KHS. Updated information will be marked with an asterisk (*).

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).

For breaches that affect **fewer than 500** individuals, a covered entity must provide the Secretary with notice annually. All notifications of breaches occurring in a calendar year must be submitted within 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://ocrnotifications.hhs.gov/

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, please provide an estimate of the number of individuals affected. As this information becomes available, an additional breach report may be submitted as an addendum to the initial report.

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 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://ocrnotifications.hhs.gov/

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, please provide an estimate of the number of individuals affected. As this information becomes available, an additional breach report may be submitted as an addendum to the initial report

- 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 60 days following the discovery of a breach and must include the same information required for the individual notice.

6.6 Burden of Proof[11]

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. 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 have in place written policies and procedures regarding breach notification, must train employees on these policies and procedures, and must develop and apply appropriate sanctions against workforce members who do not comply with these policies and procedures.

REFERENCE:

Revision 2016-05: Policy revised to comply with changes to policy 2.28-P . Updated verbiage to meet PL 14-004. Updated signatory list. **Revision 2014-03:** Policy revised to comply with DHCS/DMHC Joint Medical Audit Review 2013. Added language to contact DHCS Information Security Officer. **Revision 2012-07:** Policy revised to comply with HIPAA HITECH regulations. New sections on Notification by a Business Associate, Individual Notice, Notification Requirements of Breaches of Security and Burden of Proof. **Revision 2010-10**: Policy reviewed by Chief Compliance Officer. Revisions made pursuant to HIPAA law, as revised by HITECH. **Revision 2007-05:** Revised per DHCS/DMHC Medical Audit comments 5/13/2007. Added language to comply with MMCD Letters 06001 and 06005. **Revision 2007-03:** Revised per DHCS/DMHC Medical Audit Review Category 4.4.1 (YE 10/31/2006). **Revision 2005-03:** Revised to comply with DHCS 2004 Contract and Site Review Tool. **Revision 2003-10:** Revised to comply with HIPAA and AB700 (2002). **Revision 2002-06:** Revised per DHCS Comment 05/13/02. **Revision 2002-04:** Revised per DHCS Comment 09/19/01. **Revision 2001-06:** (*Comments received from DHCS 09/19/01. This version never implemented.*) Revised to comply with changes to the Confidentiality of Medical Information Act. Deleted policy #2.24 and incorporated information into this policy. Submission to DMHC required. **Revision 2001-02**: changes made for 2000 Legislation submission – DMHC.

[1] California Civil Code §56.101. Supported in 45 CFR §164.530(c)
[2] 45 CFR §164.526(f)
[3] Total preemption of HSC 123111 by 45 CFR §164.526 per CalOHI analysis.
[4] California Civil Code §56.101
[5] CCR Title 22 §75055(a); HSC 123145
[6] California Civil Code §56.101
[7] 45 CFR §164.502(d) and 164.514
[8] AB700 (2002) effective July 1, 2003. ; California Civil Code §1798.82
[11] Section 13402Health Information for Economic and Clinical Health (HITECH) Act