Kern County Administrative Office

County Administrative Center
1115 Truxtun Avenue, Fifth Floor • Bakersfield, CA 93301-4639
Telephone 661-868-3198 • FAX 661-868-3190 • TTY Relay 800-735-2929

ADMINISTRATIVE BULLETIN NO. 38

Issued: March 13, 2012

SUBJECT: CONFIDENTIALITY OF MEDICAL INFORMATION POLICY

It is the policy of the County to adhere to federal and State laws regulating the privacy of medical information, including but not limited to the federal Health Insurance Portability and Accountability Act (HIPAA), the federal Health Information Technology for Economic and Clinical Health Act (HITECH) and California's Confidentiality of Medical Information Act (CMIA). The County is committed to providing a confidential environment surrounding all Protected Health Information (PHI). Intentional, unauthorized access to, use of, or disclosure of PHI is strictly prohibited. Furthermore, the County cannot tolerate negligent or inadvertent disclosure of confidential information and will hold its employees to strict standards. Violations of this policy shall result in disciplinary action, up to and including termination of employment.

1. Definitions:

   a. Breach – The term "breach" means the unauthorized acquisition, access, use, or disclosure of protected health information.

   b. Intentional – Means "knowing" and "willful" as defined below.

   c. Knowing – A knowledge that the facts exist which bring the act or omission within the provisions of the law. It does not require any knowledge of the unlawfulness of such act or omission.

   d. Willful – A purpose or willingness to commit the act, or make the omission referred to. It does not require any intent to violate law, or to injure another, or to acquire any advantage.

   e. Authorized – Permission granted in accordance with Civil Code section 56.11 or 56.21 for the disclosure of medical information. Authorized access to Medical Information is generally limited to treatment, management, and billing processes.

   f. 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 or physical condition, or treatment.

   g. Protected Health Information (PHI) – Individually identifiable information relating to the past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care

provided to an individual. Individually identifiable health information may be transmitted or maintained in any form or medium, including oral, written and electronic. Information is considered PHI where there is a reasonable basis to believe the information can be used to identify an individual. PHI includes the following:

i. Names;
ii. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census:
    1. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
    2. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people are changed to 000.
iii. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
iv. Phone numbers;
v. Fax numbers;
vi. Electronic mail addresses;
vii. Social Security numbers;
viii. Medical record numbers;
ix. Health plan beneficiary numbers;
x. Account numbers;
xi. Certificate/license numbers;
xii. Vehicle identifiers and serial numbers, including license plate numbers;
xiii. Device identifiers and serial numbers;
xiv. Web Universal Resource Locators (URLs);
xv. Internet Protocol (IP) address numbers;
xvi. Biometric identifiers, including finger and voice prints;
xvii. Full face photographic images and any comparable images; and
xviii. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data).

h. Treatment, Payment and Health Care Operations (TPO) – Includes all of the following:

i. Treatment – the provision, coordination, or management of health care and related services, consultation between providers relating to an individual, or referral of an individual to another provider for health care.
ii. Payment – Activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collection activities, medical necessity determinations and utilization review.
iii. Health Care Operations – Includes functions such as quality assessment and improvement activities, reviewing competence or qualifications of health care professionals, conducting or arranging for medical review, legal services and auditing functions, business planning and development, and general business and administrative activities.

2. Acts Resulting in Prosecution and/or Disciplinary Action

    a. Any intentional act or willful conduct or omission which results in the unauthorized access to or disclosure of patient or employee medical information and or PHI as defined above by an employee in violation of HIPAA, HITECH, CMIA, or other applicable state or federal statute or regulation shall be treated as a serious violation of County policy and rules. Employees should be aware that even a single intentional, unauthorized access or disclosure may result in termination of their employment, civil penalties and/or criminal prosecution. Investigation and determination of appropriate disciplinary measures shall include but not be limited to consideration of the following:

        i. The employee's timeliness and diligence in reporting the conduct and violation(s) to management.
        ii. Whether the employee made a diligent, good faith attempt to comply with policy.
        iii. The nature and seriousness of the violations.
        iv. The harm to the patient/employee/County.
        v. The total number of violations.
        vi. The number of patient/employee records involved.
        vii. The method of access and/or disclosure.
        viii. The persistence and/or frequency of the violations.
        ix. The length of time over which the violations occurred.
        x. The willfulness of the employee's violations.
        xi. Any other facts and circumstances that the County deems relevant.

    b. Any negligent act or inadvertent conduct and/or omission which results in the access to or disclosure of patient or employee medical information by an employee in violation of HIPAA, HITECH, CMIA or other applicable state or federal statute or regulation may be treated as a serious violation of County policy and rules, which is subject to disciplinary action up to and including termination. Investigation and determination of appropriate discipline shall include but not be limited to consideration of the following:

        i. The employee's timeliness and diligence in reporting the conduct and violation(s) to management.
        ii. Whether the employee made a diligent, good faith attempt to comply with policy.
        iii. The nature and seriousness of the violations.
        iv. The harm to the patient/employee/County.
        v. The number of violations.
        vi. The number of patient/employee records involved.
        vii. The method of access and/or disclosure.
        viii. The persistence and/or frequency of the violations.
        ix. The length of time over which the violations occurred.
        x. Any other facts and circumstances that the County deems relevant.

3. Employee Responsibilities

    a. Employees shall complete job-appropriate training to help them avoid HIPAA, HITECH, CMIA or other applicable state or federal statute or regulation violations.

b. Employees shall refrain from accessing confidential medical information in violation of HIPAA, HITECH, CMIA or other applicable state or federal statutes or regulations.

c. Employees who access or disclose confidential medical information in violation of HIPAA, HITECH, CMIA or other applicable state or federal statutes or regulations must immediately report such access or disclosure to their supervisors.

d. Employees who observe and/or discover the unauthorized access or disclosure of confidential medical information in violation of HIPAA, HITECH, CMIA or other applicable state or federal statutes or regulations must immediately report such access or disclosure to their supervisors. Alternatively, unauthorized access, use, or disclosure may be reported anonymously via the County hotline.

e. Supervisors discovering improper access or disclosure must immediately report to their supervisors until the department head is aware of the violation.

4. Department Responsibilities

a. Department heads shall ensure that the County's Confidentiality of Medical Information Policy is fully implemented and shall provide job-appropriate training for all employees.

b. Upon discovery of a breach as defined above, the department must immediately report the breach to its Compliance Officer and/or County Counsel so that any reporting requirements can be met in a timely manner.

c. The department must investigate all potential breaches and ensure that appropriate disciplinary, legal, or other actions are taken.

d. Upon investigation, the department should determine the reason for the breach and determine how to prevent future violations.

e. Departments should consult with County Counsel regarding any agreement with third party vendors in which PHI and/or medical information will be shared, exchanged, accessed or transferred.