COMPLIANCE & PRIVACY BASICS

FOR HEALTH CARE PROVIDERS

Kaweah Delta

MORE THAN MEDICINE. LIFE.

COMPLIANCE & PRIVACY BASICS

KAWEAH DELTA COMPLIANCE PROGRAM

The laws and rules that apply to the delivery of healthcare can be complex and confusing; therefore, we have established a compliance program to assist with the understanding and implementation of those laws and rules.

Compliance Contacts:
Ben Cripps, Compliance and Privacy Officer
(559)624-5006

Sravan Sharma, Compliance Manager
(559)624-5029

Compliance Department
(559)624-2154

Anonymous Compliance Line:
1(800)998-8050

MEDICAL RECORD DOCUMENTATION

Payers trust you, as a physician, to provide necessary, cost-effective, and quality care. You exert significant influence over what services your patients receive, you control the documentation describing what services they actually received, and your documentation serves as the basis for bills sent to insurers for services you provided. The Government's payment of claims is generally based solely on your representations in the claims documents.
It is vital to patient care and compliance with Federal and State law that medical records contain current and accurate documentation.

Examples:

- A cardiologist paid $435,000 and entered into a 5-year Integrity Agreement with OIG to settle allegations that he knowingly submitted claims for consultation services that were not supported by patient medical records and did not meet the criteria for a consultation.

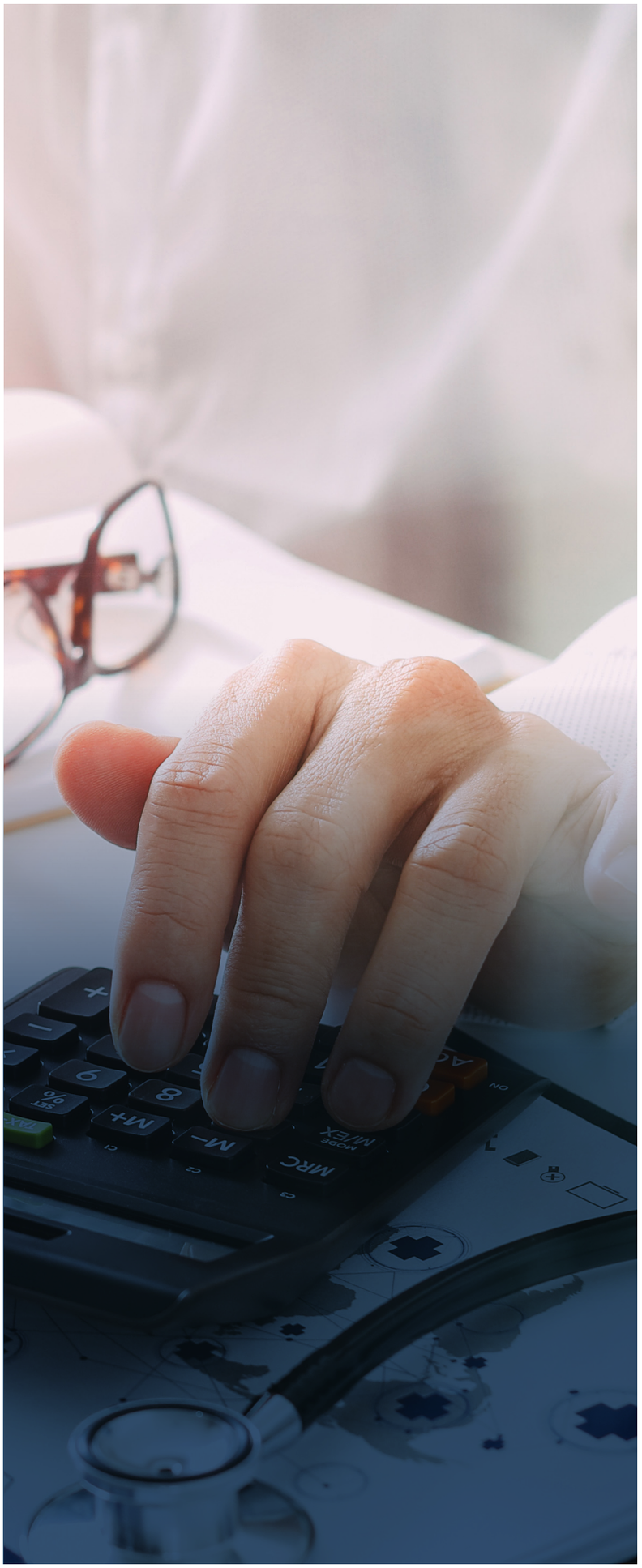
- A psychiatrist was fined $400,000 and permanently excluded from participating in the Federal health care programs for misrepresenting that he provided therapy sessions requiring 30 or 60 minutes of face-to-face time with the patient, when he had provided only medication checks for 15 minutes or less. The psychiatrist also misrepresented that he provided therapy sessions when in fact a non-licensed individual conducted the sessions.

ACCURATE CODING AND BILLING

When you submit a claim for services performed for a Medicare or Medicaid beneficiary, you are filing a bill with the Federal Government and certifying that you have earned the payment requested and complied with the billing requirements. If you knew or should have known that the submitted claim was false, then the attempt to collect unearned money constitutes a violation. A common type of false claim is "upcoding," which refers to using billing codes that reflect a more severe illness than actually existed or a more expensive treatment than was provided.

Examples:

- E&M coding and lack of documentation
- Billing for services that you did not actually render
- Billing for services that were not medically necessary
- Billing for services that were performed by an improperly supervised or unqualified employee
- Billing separately for services already included in a global fee
- Billing for an evaluation and management service the day after surgery



COMPLIANCE & PRIVACY BASICS

ANTI-KICKBACK STATUTE (AKS)

The AKS is a criminal law that prohibits knowingly and willfully offering, paying, soliciting or receiving any money gifts, kickbacks, bribes, rebates or any other type of value or services in exchange for the referral of patients for which payment may be made by the federal or state government.

Examples:

- Free or significantly discounted billing, nursing care, rent or other staff services
- Payment for services in excess of Fair Market Value
- Payment or other type of incentive when a patient is referred to Kaweah Delta

PHYSICIAN SELF-REFERRAL LAW ("STARK LAW")

The Physician Self-Referral Law, commonly referred to as the Stark law, prohibits physicians from referring patients to receive "designated health services" payable by Medicare or Medicaid from entities with which the physician or an immediate family member has a financial relationship, unless an exception applies. Financial relationships include both ownership/investment interests and compensation arrangements. The Stark law is a strict liability statute, which means proof of specific intent to violate the law is not required. The Stark law prohibits the submission, or causing the submission, of claims in violation of the law's restrictions on referrals. Penalties for physicians who violate the Stark law include fines as well as exclusion from participation in the Federal health care programs.

Examples:

- Paying doctors in ways that rewarded them financially for referring patients to the hospital
- Entering into favorable leases with physicians who referred patients to the hospital
- If you invest in an imaging center you may not refer patients to the facility and the entity may not bill for the referred imaging services Agreement unless an exception applies

EXCLUSION STATUTE

The Office of Inspector General (OIG) is legally required to exclude from participation in all Federal health care programs individuals and entities convicted of the following types of criminal offenses: (1) Medicare or Medicaid fraud, as well as any other offenses related to the delivery of items or services under Medicare or Medicaid; (2) patient abuse or neglect; (3) felony convictions for other health-care-related fraud, theft, or other financial misconduct; and (4) felony convictions for unlawful manufacture, distribution, prescription, or dispensing of controlled substances. Kaweah Delta is responsible for ensuring that we do not employ or contract with excluded individuals or entities. Kaweah screens all current and prospective physicians against OIG's List of Excluded Individuals and Entities.

Example:

- Excluded physicians may not bill directly for treating Medicare and Medicaid patients, nor may their services be billed indirectly through an employer or a group practice.

FRAUD, WASTE AND ABUSE

Violation of federal and state laws concerning fraud and abuse can result in significant criminal and civil penalties, including imprisonment, fines, and damages. You must be vigilant in avoiding any conduct that could violate or even appear to violate these laws.

Fraud:
Obtaining a benefit through intentional misrepresentation or concealment of material facts.

Waste:
Includes incurring unnecessary costs as a result of deficient management, practices, or controls.

Abuse:
Includes excessively or improperly using resources.

Examples:

- Claiming reimbursement for items or services that were not provided as claimed

- Failing to maintain sufficient documentation to establish that the services were ordered and performed

PATIENT PRIVACY

HIPAA is the Health Insurance Portability and Accountability Act of 1996. HIPAA is a suite of regulations including the ***Privacy Rule,*** which protects the privacy of individually identifiable health information; the ***Security Rule***, which sets national standards for the security of electronic Protected Health Information (ePHI); and the ***Breach Notification Rule,*** which requires governs notification requirements following a breach of unsecured PHI. Whether patient health information is on a computer, in an Electronic Health Record (EHR), on paper, or in other media, providers have responsibilities for safeguarding the information by meeting the requirements of the Rules.

Who must comply with the HIPAA Rules?
Covered Entities (CE) and Business Associates (BA) must comply with the HIPAA Rules.

CEs include:
- Health care providers who conduct certain standard administrative and financial transactions in electronic form, including doctors, clinics, hospitals, nursing homes, and pharmacies. Any health care provider who bills electronically (such as a current Medicare provider) is a CE.

- Health plans

- Health care clearinghouses

What types of information does HIPAA protect?
The Privacy Rule protects most individually identifiable health information held or transmitted by a , in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information" or "PHI." Individually identifiable health information is information, including demographic information that relates to:

- The individual's past, present, or future physical or mental health or condition,

- The provision of health care to the individual, or

- The past, present, or future payment for the provision of health care to the individual

In addition, individually identifiable health information can be when there is a reasonable basis to believe it can be used to identify the individual.

Example:
- A medical record, laboratory report, or hospital bill would be PHI if information contained therein includes a patient's name and/or other identifying information.

Use and Disclosures of PHI:
In general, you as a provider may use and disclose PHI for treatment, payment, and health care operations activities — and other permissible or required purposes consistent with the HIPAA Privacy Rule — without obtaining a patient's written permission (e.g., consent or authorization).

You also may disclose PHI for:
- The treatment activities of another health care provider,

- The payment activities of another health care provider, or

- The health care operations of another Covered Entity (CE) when:

  - Both CEs have or have had a relationship with the individual

  - The PHI pertains to the relationship

  - The data requested is the minimum necessary

  - The health care operations are:

- Quality assessment or improvement activities
- Review or assessment of the quality or competence of health professionals, or

- Fraud and abuse detection or compliance

When Are Patient Authorizations Not Required for Disclosure?

• ***Information Sharing Needed for Treatment*** – You may disclose, without a patient's authorization, PHI about the patient as necessary for treatment, payment, and health care operations purposes. Treatment is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another. A disclosure of PHI by one CE for the treatment activities undertaken by another CE is fundamental to the nature of health care.

• ***Disclosures to Family, Friends, and Others Involved in the Care of the Individual as well as for Notification Purposes*** – To make disclosures to family and friends involved in the individual's care or for notification purposes, or to other persons whom the individual identifies, you must obtain informal permission by asking the individual outright, or by determining that the individual did not object in circumstances that clearly gave the individual the opportunity to agree, acquiesce, or object. For example, if a patient begins discussing health information while family or friends are present in the examining room, this is a "circumstance that clearly gave the individual the opportunity to agree, acquiesce, or object." You do not need a written authorization to continue the discussion.

- Where the individual is incapacitated, in an emergency situation, or not available, a CE generally may make such disclosures, if the provider determines through his/her professional judgment that such action is in the best interests of the individual

- You must limit the PHI disclosed to what is directly relevant to that person's involvement in the individual's care or payment for care. Similarly, a CE may rely on an individual's informal permission to use or disclose PHI for the purpose of notifying (including identifying or locating) family members, personal representatives, or others responsible for the individual's care, of the individual's location, general condition, or death.

• ***Information Needed to Ensure Public Health and Safety*** – You may disclose PHI without individual authorization in the following situations:

- To 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. This would include, for example, the reporting of disease or injury; reporting vital events, such as births or deaths; and conducting public health surveillance, investigations, or interventions

- To persons at risk of contracting or spreading a disease or condition if other law, such as state law, authorizes the CE to notify such individuals as necessary to prevent or control the spread of the disease.

• ***Information Needed to Prevent or Lessen Imminent Danger*** – You may disclose PHI that you believe is necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone you believe can prevent or lessen the threat (including the target of the threat). CEs may also disclose to law enforcement if the information is needed to identify or apprehend an escapee or violent criminal.

When Are Patient Authorizations Required for

Disclosure?
A CE must obtain the individual's written authorization for any use or disclosure of PHI that is not for treatment, payment, or health care operations or otherwise permitted or required by the Privacy Rule. A CE may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances.

Specific purposes that require an individual's written authorization include:

- Psychotherapy Notes – Your practice and your BA must obtain an individual's authorization to use or disclose psychotherapy notes with the following exceptions:

  - The CE who originated the notes may use them for treatment.

  - A CE may use or disclose, without an individual's authorization, the psychotherapy notes for its own training; to defend itself in legal proceedings brought by the individual; for HHS to investigate or determine the CE's compliance with the Privacy Rules; to avert a serious and imminent threat to public health or safety; to a health oversight agency for lawful oversight of the originator of the psychotherapy notes; for the lawful activities of a coroner or medical examiner; or as required by law.

- Research – Special rules apply with regard to clinical research, bio-specimen banking, and all other forms of research not involving psychotherapy notes. In some circumstances, patient authorization is required. You may want to obtain specific guidance on these requirements from the Kaweah Delta Office of Research.

Examples:

Being overheard discussing PHI.
Whether it's leaving a detailed message on a patient's answering machine or discussing test results with a patient in the waiting room, be aware of who else may be listening to your voice. Do not to leave PHI in phone messages and do not to discuss it within earshot of other patients or non-staff visitors. When possible, use private rooms for health discussions with patients as well as phone conversations that could involve PHI.

Encryption
The best way to protect devices such as thumb drives, tablets, and laptops from a breach is to have an IT professional encrypt the device. If the device is lost or stolen, this process makes it very difficult for an unauthorized person to access the data. When encrypted, a lost or stolen device does not have to be reported to the government as a breach of unsecured equipment—because it was secured through encryption.

Snooping in Healthcare Records.
University of California Los Angeles Health System was fined $865,000 for failing to restrict access to medical records. The healthcare provider was investigated following the discovery that a physician had accessed the medical records of celebrities and other patients without authorization. Dr. Huping Zhou accessed the records of patients without authorization 323 times after learning that he would soon be dismissed. Dr. Zhou became the first healthcare employee to be jailed for a HIPAA violation and was sentenced to four months in federal prison.

RELEASING PHI TO LAW ENFORCEMENT

Hospitals and health systems are responsible for protecting the privacy and confidentiality of their patients and patient information. Health Insurance Portability and Accountability Act (HIPAA) prohibits the release of information without authorization from the patient except in the specific situations identified within the regulations. We have included examples of a few situations that you may encounter at Kaweah Delta. This is not a comprehensive list of all scenarios, as such; please reach out to Risk Management at 559-624-2340 or Compliance at 559-624-2154 if you need assistance.

When May A Hospital Disclose Information To A Law Enforcement Official?

HIPAA and state laws allow hospitals to disclose protected health information to law enforcement officials for certain limited purposes without patient authorization. In some cases, the law enforcement official must initiate the request for information and in other cases the hospital may report information without a law enforcement request.

The Lanterman-Petris-Short (LPS) Acts states that information released from a Psychiatric Hospital or related to a patient on a psychiatric hold such as a 5150, 5250, or 1799 hold may only be disclosed to third parties with permission of the client and approval from the provider.

Disclosures Permitted Without Authorization Required:

HIPAA permits hospitals to disclose patient information for reporting purposes that are required by law. For example, LPS patient escapes, abuse & neglect, and death may be disclosed to the extent the report is required by law and limited to relevant requirements of the law.

Compliance Advice:

- When the law permits you to release information to law enforcement, it improves relationships if you do so in a helpful way that protects privacy while still helping "in the interests of justice".

- Always consider asking the patient for permission first when the law allows the release with the patient's written permission.

SITUATION	ALL PATIENTS
Disclosures of limited patient information or to assist in identifying or locating a patient:	
PATIENT IS PRESENT AND ABLE TO MAKE DECISIONS	Yes, if you obtain verbal confirmation from the patient or provide an opportunity for the patient to object, or reasonably infer that patient does not object.
PATIENT IS INCAPACITATED OR EMERGENCY SITUATION	You are permitted to disclose limited information if in the provider's professional judgement, they determines that disclosure is in the best interest of patient. However, you may only disclose PHI needed for notification purposes (minimum necessary).
KD Policy: AP107	
Law Enforcement Official **REQUESTS INTERVIEW WITH PATIENT** KD Policy: AP07	Yes if you obtain patient verbal agreement **AND:** 1. Must contact Risk Management, the House Supervisor, or Compliance; **AND** 2. Advise patient of any adverse medical consequences. ***If patient objects,*** and officer persists, escalate the situation to officer's supervisor as the stress could affect the patient's medical condition. Never attempt to physically prevent an officer from interrogating a patient.

MENTAL HEALTH/PSYCHIATRIC HOLD PATIENT	
Yes, if you obtain verbal confirmation from the patient. If patient objects, you cannot release information. You are prohibited from even confirming/denying patient is present within the facility.	
You may not disclose PHI unless the request for information is made by the spouse, parent, child or sibling of the patient and the patient is unable to authorize the release of information. Under these circumstances, the spouse, parent, child or sibling of the patient must be notified of the patient's presence in the facility.	
NOTE: You must document daily attempts to secure the patient's authorization or refusal.	
Yes if you obtain patient verbal agreement **AND:** 1. Must contact Risk Management, the House Supervisor, or Compliance; **AND** 2. Advise patient of any adverse medical consequences. ***If patient objects, you cannot release information.*** You are prohibited from even confirming/denying patient is present. Limited disclosure is permitted if the patient is in a locked psychiatric facility and law enforcement asks if patient is there ***and has an arrest warrant for violent or serious felony.***	

SITUATION
REQUEST TO DIRECT TREATMENT (Ex. Lab Draw, Specimens, etc.)
ALL PATIENTS **MENTAL HEALTH/PSYCHIATRIC HOLD PATIENT**
A request from law enforcement to direct treatment involving a prisoner requires: • Patient Consent; or • Consent from a surrogate decision maker on behalf of the patient if patient is unconscious or incapacitated; or • Court order In general, a patient doesn't lose his or her right to or refuse consent to medical care just because he or she is in custody.


Social Media
56
Facebook
Instagram
102
WhatsApp
1
1
Snapchat
Twitter
1
YouTube
383
Gmail

SOCIAL MEDIA

When using social media consider the following guidelines to ensure you do not violate HIPAA regulations.

- While you may be concerned about seeming unfriendly, limiting your social media interactions to friends and family members is prudent. This will protect you from having patients ask questions regarding their personal health on a public forum and help you to avoid disclosing the names of patients you treat.

- Avoid talking about patients, even in general terms. Even if disclosure of PHI is unintentional it is still a violation of HIPAA.

- Avoid posting photos of patients or anything that could be used to identify them (notes, lab results, etc.)

- Periodically check your privacy settings, as they can change.

- Never post anything that you would be uncomfortable reading re-printed in the newspaper. This can be a helpful test to take before you hit the 'send' button.

Examples:

- An obstetrician vents her frustrations on her online blog, ridiculing the patients giving birth. Although the physician did not use patient names or any other identifying information in her post, two of the patients recognized themselves in the blog due to the detailed nature of the post and filed HIPAA complaints against the doctor and the practice.

- An ED physician in Rhode Island was fired, lost her hospital medical staff privileges, and was reprimanded by the Rhode Island Board of Medical Licensure and Discipline for posting information about a trauma patient on her personal Facebook page.

According to the Rhode Island Board of Medical Licensure and Discipline, "[She] did not use patient names and had no intention to -reveal any confidential patient information. However, because of the nature of one person's injury … the patient was identified by unauthorized third parties. As soon as it was brought to [her] attention that this had occurred, [she] deleted her Facebook account." Despite the physician leaving out all information she thought might make the patient identifiable, she apparently did not omit enough.

References:
1. MEDICAL PRIVACY OF PROTECTED HEALTH INFORMATION, https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/downloads/SE0726FactSheet.pdf
2. HIPAA BASICS FOR PROVIDERS: PRIVACY, SECURITY, AND BREACH NOTIFICATION RULES, https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurity.pdf
3. Your Practice and the HIPAA Rules, https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide-chapter-2.pdf

COMPLIANCE & PRIVACY BASICS

FOR HEALTH CARE PROVIDERS

KAWEAHDELTA.ORG

Kaweah Delta
MORE THAN MEDICINE. LIFE.