PROFESSIONAL FEE BILLING: NEW TRAINING MODULES

Two new training modules related to professional fee billing matters are available. The first module, Critical Care—Coding and Billing Guidance can be accessed on the UC Learning Center (key word: "Proftee"), and has been assigned for completion by all physicians who bill critical care services. Under this module, you will learn about the definition and criteria of critical care and other E/M services including the appropriate documentation and billing examples.

Additionally, the Inpatient Admission & Medical Necessity training module will be available on the UC Learning Center in January. This course will be assigned for completion to all medical staff members with active privileges and GME residents. This module will review medical necessity, inpatient admission versus observation services, the Two Midnight Rule, and documentation requirements.

Although the courses have been assigned for specific populations, the modules are available to all employees, and we encourage you to review at your convenience.

REPORTING COMPLIANCE CONCERNS

Workforce members are our first line of defense in detecting and preventing violations and all workforce members are obligated to report actual or suspected violations. Always seek advice when you are not sure about the right ethical or legal thing to do. Do not guess whether a particular action is permitted.

UC San Diego Health Sciences absolutely prohibits retaliation against any workforce member who raises a compliance concern in good faith. Retaliation towards a workforce member who raises a compliance concern in good faith is subject to disciplinary action, up to and including termination.

If you believe someone has retaliated against you for raising a compliance concern, notify the Compliance Officer (858.657.7487) or call the UC Hotline immediately (800.403.4744).
Although you may want to access your family member’s medical information in a quicker manner (or believe you are entitled to it as the patient’s parent/guardian), accessing UCSDH Epic Electronic Health Record may be a violation of patient privacy policies – and could result in further disciplinary actions to YOU! But, the federal privacy rules recognize the role of family members who are involved in the patient’s care and provided other options to facilitate necessary information sharing in a manner that protects the patient’s privacy while permitting necessary communications.

Consider these options:
With the patient’s prior written authorization, you may request a copy of the patient’s medical record from Health Information Management (HIM) office. Form #151-036 or refer to HIM’s web page: http://health.ucsd.edu/patients/Pages/medical-records.aspx

If you are the patient’s “Designated Personal Representative”, you may request a copy of the patient’s medical information and also speak to the patient’s care team. Form #D1031, Designation of Personal Representative. http://forms.ucsd.edu

If you are the patient’s “health care power-of-attorney” (HC-POA), then you have the ability to act for the patient and exercise certain individual rights regarding access to the medical record. However, the method for access is in the same manner as for other patient requests by going through Health Information Management. You may be asked to provide a copy of the signed HC-POA form for filing in the patient’s record.

The patient may view their own results via MyUCSDChart. https://myucsdchart.ucsd.edu/

As a treating provider, if in your judgment the family member or friend is involved in the patient’s ongoing care, you may disclose the minimum necessary information to facilitate continuity of care. Refer to the OCR’s guide on this topic.

To learn more:


PRIVACY REMINDERS

**Meeting Agendas.** Adhere to the minimum necessary standard. Do not include patient identified protected health information (PHI) or other restricted information in electronic meeting agendas distributed via unencrypted email. Provide a link to a secure site to view information that is necessary for the meeting and limit the distribution to authorized meeting participants.

**Email Distribution Lists.** Regularly review and update email distribution lists. Review email lists at least annually and when staffing personnel actions occur that impact distribution lists, e.g., new hire, separation, extended leave without pay, transfers to another department, retirement, job changes. If you are notified of wrong recipient on an email containing restricted information, notify the Privacy Office promptly.
HIPAA PRIVACY VIOLATIONS AND SOCIAL MEDIA

Under HIPAA regulations, it is illegal for health care providers to share patient’s diagnosis and treatment information without patient permission. The Office for Civil Rights is responsible for enforcing HIPAA laws, and receives in excess of 30,000 reports of privacy violations annually.

Most HIPAA breaches that make the news are large in scale, with hackers accessing large databases containing patient information. However, the impact of such privacy breaches extends beyond these large-scale database breaches. These very personal and costly breaches often occur by sharing patient information on social media. Recently, UCLA was sued by a patient alleging a privacy violation by a temporary worker who accessed the patient’s medical records as part of an ex-lover’s quarrel.

In recent years, hospital staff across the country have run afoul of HIPAA by posting photos and/or identifying information about patients on various social media outlets. Although not intentional or malicious acts, any time a patient’s medical information is shared without his or her permission, the breach has already occurred. Even if the patient is not identified by name or medical record number, the information you disclose may identify the patient and be deemed a breach.

Although small in scale, the impact on the individual patient can be immense. As a result, it is imperative to be cognizant of the information you share. For more information on the Privacy trainings and resources available to UCSD Health employees, please see below. To review the local policy on social media guidelines, see MCP 523.1.

PRIVACY RESOURCES FOR UCSD HEALTH

UCSD Health Sciences Compliance Program is committed to actively educating our faculty and staff on the rules and implications of HIPAA. All UCSD Health employees are required to complete mandatory compliance trainings each year. Completion of the 2015 Annual Compliance Training was due on or before June 26, 2015 for all UCSD Health employees and faculty (including Medical Center and Professional School employees). If you have yet to complete the required training, please log-in to UCLearning as soon as possible to complete your training. Once logged in, you can access the module by searching for “2015 Annual Compliance Training” if you are not already registered for the course. Any questions on registration can be directed to Tamitha Mueller, Learning Management System Specialist, at trmueller@ucsd.edu.

Vigilance in preventing privacy breaches starts with our employees. In addition to the trainings offered, there are multiple resources available to assist with related topics, including encryption of personal devices which may be used to access PHI. See the June 2015 Compliance Newsletter for guidance on your responsibility for protecting your devices. As a reminder, details on how to secure your mobile device can be accessed on Blink here and also at UCSD HS Information and Technology.

If you or someone you know has reason to believe that a privacy violation may have occurred, please contact Cheryl Nikas, Privacy Program Manager, at (858) 657-7487 or via email at hscomply@ucsd.edu.
INFORMATION SECURITY RESOURCES

Computer and Network Security

UCSD Network Security

Identify Phishing Scams

Cloud Security and Your Data

INFORMATION SECURITY SERVICES:
SECURITY IN THE NEWS

Information Security Services – Security in the news!

HIPAA Settlement reinforces lessons for users of medical devices, November 25, 2015

Lahey Hospital and Medical Center, a teaching hospital in Burlington, Massachusetts was fined $850,000 by the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) for non-compliance with HIPAA privacy and security rules. Lahey notified OCR that a laptop was stolen from an unlocked treatment room during overnight hours in August 2011. The laptop was on a stand that accompanied a portable CT scanner for Lahey’s Radiology Information System and Picture Archiving and Communication System. The laptop hard drive contained the protected health information (PHI) of 599 individuals. In addition to the impermissible disclosure of ePHI for 599 individuals, OCR’s subsequent investigation indicated other non-compliance with the HIPAA rules.

HHS HealthIT.gov offers tips on how to protect and secure health information when using mobile devices: https://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security “Mobile Devices: Know the Risks, Take the Steps, Protect & Secure Health Information”

UCSDH Information Security Services, http://mcit.ucsd.edu

Computer Security

Refer to Chancellor Khosla’s all academic and staff email sent July 17, 2015 regarding computer security.

All mobile devices and removable media must be encrypted and password protected regardless of whether or not the device is used to access or store restricted information. Encrypt all devices now. Additionally, any transfer of data containing restricted information must be transferred using cryptographic methods. Ask your IT support group for help or learn more at the link below.

For information to obtain Sophos antivirus software and full disk encryption software, please visit: http://blink.ucsd.edu/technology/security/network/standards/resources.html and http://mcit.ucsd.edu.

USB storage devices must all be encrypted. For help encrypting your devices contact UC San Diego Health Information Services at (619) 543-7474.
PROFESSIONAL FEE BILLING:
CRITICAL CARE SERVICES

Key Points & Requirements

Critical Care – Defined:
Critical care is defined as urgent medical care that is delivered directly by a physician(s) where the nature of the patient’s condition is critical due to illness or injury. A critical illness or critical injury is one that acutely impairs one or more vital organ systems in such a way there is a high probability of imminent or life threatening deterioration in the patient’s condition.

Billing Criteria:

**Critical Patient.** The patient must be critically ill or critically injured. The provider must treat the critical illness using “high complexity decision making to assess, manipulate, and support vital systems to treat single or multiple vital organ system failure and/or prevent further life threatening deterioration of the patient’s condition. The care must be medically necessary in the treatment or management of a patient’s imminent deterioration condition. AND

**Time.** The clinician also must spend at least 30 minutes providing critical care. Time spent may be either continuous or intermittent, then aggregated and measured from midnight to midnight each day. Care must be provided at the bedside or on the floor/unit where the patient is housed.

**Documentation of both elements.** As long as (1) the nature of the patient’s condition for care meets the definition of critical care, and (2) the time spent is at least 30 minutes or more, then the CPT codes for critical care may be billed by the attending physician (or other authorized clinical provider who is credentialed for professional fee billing). Documentation for each date must reflect both criteria in the patient’s medical record as well as the teaching physician billing rules to support billed services.

TO ACCESS THE COMPLETE FACTSHEET, PLEASE CLICK HERE.
CMS Two-Midnight Enforcement Delay Extension

CMS has announced it extended its enforcement delay of the Two-Midnight Rule from September 30, 2015 to January 1, 2016.

Under the Two-Midnight Rule, Medicare’s payment and audit contractors are to assume the legitimacy of a hospital admission if it spans two midnights, with shorter stays assumed to be more appropriately billed as outpatient observation care.

For more information on the Two-Midnight Rule and the delayed enforcement, click here.