HIPAA: Handling Patient Requests

for Medical Record Restriction

Healthcare compliance professionals frequently face confusing situations about sharing of protected health information (PHI). The Health Insurance Portability and Accountability Act (HIPAA) supports the protection of privacy of medical records. However, even when a patient does not authorize sharing of his record, there are permitted uses and disclosures, such as for the purpose of treatment, payment, or healthcare operations (TPO).

The U.S. Department of Health and Human Services (HHS) Office of the National Coordinator for Health IT (ONC) and the Office for Civil Rights (OCR) provide a series of topical fact sheets on HIPAA Permitted Uses and Disclosures with examples of when PHI can be exchanged under HIPAA without first requiring a specific authorization from the patient. Please note that state laws may also apply.

Permitted Uses and Disclosures for Health Care Operations

The ONC issued a useful fact sheet explaining Permitted Uses and Disclosures for Health Care Operations. For activities that fall within HIPAA's definition of "healthcare operations," an entity covered by HIPAA (Covered Entity), such as a physician or hospital, can disclose PHI to another Covered Entity (or a contractor working for that covered entity, i.e., Business Associate).

A Covered Entity (CE) can disclose PHI (orally, on paper, by fax, or electronically) to another CE or that CE's Business Associate for the following subset of healthcare operations activities without needing patient consent or authorization:

- Conducting quality assessment and improvement activities
- Developing clinical guidelines
- Conducting patient safety activities as defined in applicable regulations
- Conducting population-based activities relating to improving health or reducing healthcare cost
- Developing protocols
- Conducting case management and care coordination (including care planning)
- Contacting healthcare providers and patients with information about treatment alternatives
- Reviewing qualifications of healthcare professionals
- Evaluating performance of healthcare providers and/or health plans
- Conducting training programs or credentialing activities
- Supporting fraud and abuse detection and compliance programs 45 CFR 164.501; 45 CFR 164.506(c)(4).

Three conditions must be met when sharing PHI for the purposes stated above:

1. Both CEs must have or have had a relationship with the patient (can be a past or present patient);
2. The PHI requested must pertain to the relationship; and
3. The discloser must disclose only the minimum information necessary for the healthcare operation at hand.

What is meant by the term "minimum necessary"?

Covered entities are required to have reasonable minimum necessary policies and procedures to limit how much PHI is used, disclosed, and requested for certain purposes. Minimum necessary policies and procedures must also reasonably limit who within the entity has access to PHI, and under what conditions, based on job responsibilities and the nature of the business. For example, the minimum necessary standard requires that a CE limit who within the entity has access to PHI, based on who needs access to perform their job duties. If a hospital employee is allowed to have routine, unimpeded access to patients' medical records, where such access is not necessary for the employee to do his job, the hospital is not applying the minimum necessary standard. Therefore, any incidental use or disclosure that results from this practice, such as another worker overhearing the hospital employee's conversation about a patient's condition, would be an unlawful use or disclosure under the HIPAA Privacy Rule.

Minimum necessary standard is not required among physicians discussing a patient's medical chart for treatment purposes and does not apply to disclosures, including oral disclosures, among healthcare providers for treatment purposes.

Permitted Uses and Disclosures for Treatment

The fact sheet titled "Permitted Uses and Disclosures: Exchange for Treatment" explains how HIPAA supports sharing of PHI between and among healthcare providers in order to treat or coordinate care for their patients. CEs may disclose PHI (orally, on paper, by fax, or electronically) to another provider for the treatment activities of that provider, without needing patient consent or authorization. 45 CFR 164.506(c)(2). Treatment is broadly defined to include:

- the provision, coordination, or management of healthcare and related services by one or more providers, including the coordination or management of healthcare by a provider with a third party;
- consultation between providers relating to a patient; or
- the referral of a patient for care from one provider to another. 45 CFR 164.501.

The disclosing CE is responsible for the PHI until recipient CE has received the information. HIPAA requires disclosing the PHI to the receiving CE in a permitted and secure manner, which includes sending the PHI securely and taking reasonable steps to send it to the right address. The receiving CE is responsible for safeguarding the PHI and otherwise complying with HIPAA, including with respect to subsequent uses or disclosures or any breaches that occur.

Common HIPAA Questions

How should we ensure that we're staying compliant with HIPAA Privacy and Security Rules when sharing PHI for purposes of treatment or operations?

Many issues are covered under HIPAA Privacy and Security. Here are a few important reminders regarding permitted uses and

EXPIRING CEU ALERT

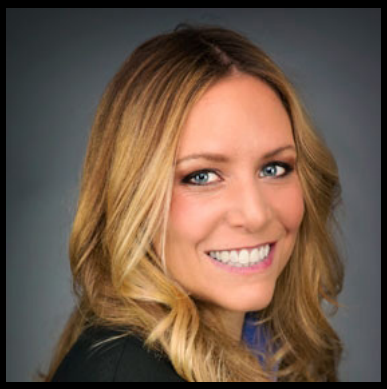
Please complete before: 09/30/2018

HIPAA Breach and What Do I Do?

Presented by: Jennifer Kirschenbaum, Esq

Length: 60 Minutes
Cost: FREE to all members

Objective: Review federal laws regarding HIPAA and the recent enforcement actions taken by OCR



Topics Covered: HIPAA, Compliance

Please visit www.billing-coding.com to access this webinar

1st Healthcare® Compliance

disclosures:

- HIPAA Security Rule compliance requires disclosure of electronic PHI by CEHRT.
- Address permitted uses and disclosures in your Notice of Privacy Practices.
- Follow minimum necessary policies and procedures and apply reasonable safeguards, as required by 45 CFR 164.502(a)(1)(iii).

What are the reasonable safeguard requirements?

Reasonable safeguards vary from CE to CE depending on factors, such as the size of the CE and the nature of its business. In implementing reasonable safeguards, CEs should analyze their own needs and circumstances, such as the nature of the PHI it holds, and assess the potential risks to patients' privacy. CEs should also consider the potential effects on patient care and may consider other issues, such as the financial and administrative burden of implementing particular safeguards.

Consider the following examples of appropriate administrative, technical, and physical safeguards:

- Sign in sheet information is limited to the patient's name, time of arrival, and the patient's doctor
- Fax machine is in a secure location and the "fax disclaimer" is on all outgoing faxes
- The Notice of Privacy Practices is on your website and there is no way to access PHI on that site
- All computer screens are turned away from the patient's view
- Screen savers are set to go on after a short period of inactivity
- No employee leaves his or her computer unattended while PHI is visible on the screen
- Passwords are assigned only to those who should have access to PHI on the computers
- Limit the information disclosed over a facility's public announcement system to the minimum necessary
- Outgoing mail only shows the minimum necessary information
- All correspondence containing PHI that is received or sent from the facility is marked confidential
- Signs are posted to restrict patient access to particular areas and to remind employees about confidentiality
- Talk quietly and do not use the full name of the patient if not necessary and always use minimum necessary when discussing in public areas
- E-mail "disclaimer" is on all outgoing messages
- Medical charts on exam room doors should be turned inward so they do not have any visible information
- Medical records are set face down when not in use

To gain more HIPAA insight and practical tips, consider purchasing The Fundamentals, a user friendly, four-module course designed to help healthcare professionals understand the essential principles and practices of compliance.

Julie Sheppard, BSN, JD, CHC, is the president and founder of 1st Healthcare Compliance. With the increase in compliance challenges facing healthcare providers, Julie was inspired to create a practical, comprehensive healthcare compliance solution, and founded First Healthcare Compliance in 2012. Julie is a nurse, an attorney, and certified in Healthcare Compliance by the Compliance Certification Board. www.1sthcc.com