McGUIREWOODS

CREATING A CULTURE OF QUALITY:

Pursuing Excellence in Care Transitions
Enhancing Safety in Kidney Patient Care

LEGAL CONSIDERATIONS TO SAFE TRANSITIONS

James B. Riley, Jr.
McGuireWoods LLP
77 W. Wacker, Suite 4100
Chicago, IL 60601-1818
(312) 750-8665
jriley@mcguirewoods.com

"Quality is never an accident; it is always the result of high intention, sincere effort, intelligent direction and skillful execution; it represents the wise choice of many alternatives."

~William A. Foster

I. Patient Transition Situations with Legal Implications
II. HIPAA and State Privacy Laws
III. Legal Implications of other Transitional Circumstances

A. Transitions from/to Renal Dialysis Facilities

- The transferring facility
- The receiving facility

B. Transitions from/to Hospitals

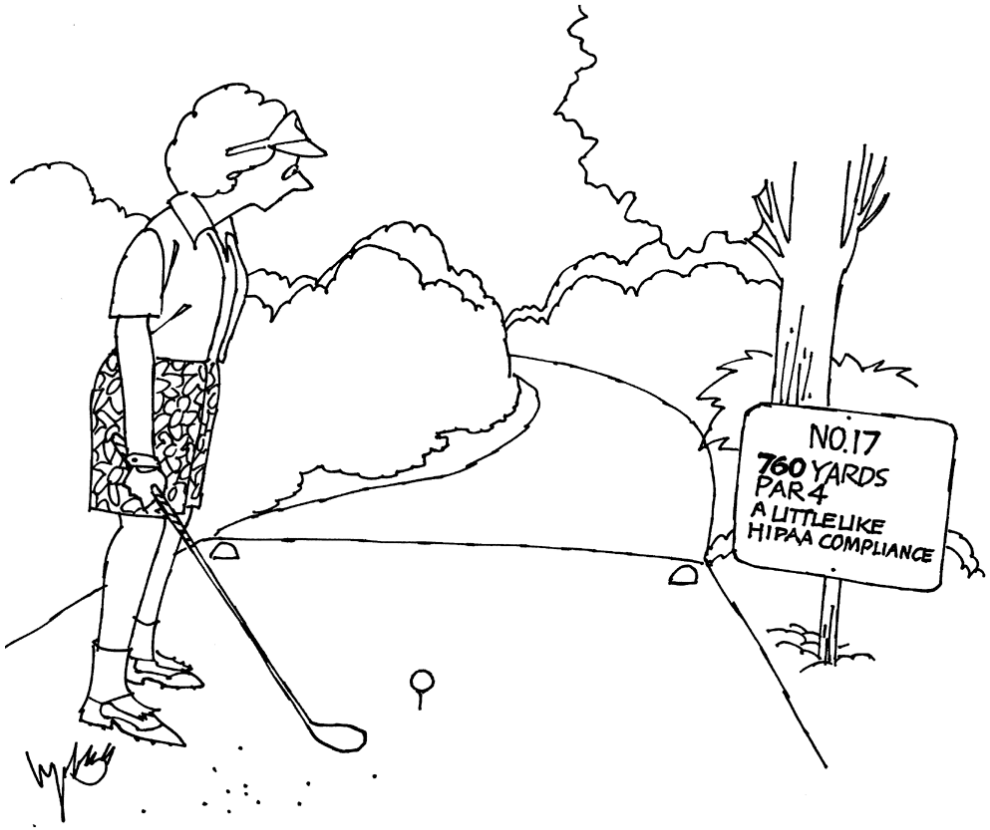
- The transferring facility/hospital
- The receiving facility/hospital

A. HIPAA and CFC Requirements in Transitioning of Patients

Conditions for Coverage for ESRD Facilities

494.170(a) Standard: Protection of the Patient's Record.

494.170(d) Standard: Transfer of Patient Record Information.



Health Insurance Portability and Accountability Act of 1996 ("HIPAA")

HIPAA mandated the enactment of the privacy and security regulations now referred to as the Privacy Rule and the Security Rule.

The Privacy Rule became effective on April 14, 2003. The Privacy Rule sets national standards for the use and disclosure of protected health information ("PHI").

The Security Rule became effective on April 20, 2005. The Security Rule sets national standards for protecting the confidentiality, integrity and availability of electronic PHI ("EPHI") when it is stored, maintained or transmitted.

The Final Rule regarding HIPAA enforcement became effective on March 16, 2006 and has been amended by the HITECH Act.

The Privacy and Security Rules apply to "Covered Entities"

- providers;
- health plans; and
- health care clearinghouses.

PHI is identifiable health information that is transmitted or maintained in any form or medium, such as:

- electronic records
- paper or other hard copies of data
- orally transmitted

Treatment, Payment or Healthcare Operations ("TPO")

- The Privacy Rule does not require a provider to obtain consent from a patient to use or disclose PHI for treatment, payment or health care operations.
- Covered entities should take reasonable steps to limit the use or disclosure to the "minimum amount necessary" to accomplish the purpose of the use or disclosure.

Exceptions: (a) treatment;

(b) to the patient; and

(c) pursuant to an authorization.

Business Associate Agreements ("BAA")

- Except as provided below, a BAA is required in order to disclose PHI to an individual or entity who is not a "member of the covered entity's workforce" to provide services "on behalf of" the covered entity.
- A BAA is not required in order for a covered entity to disclose PHI for the purposes of treatment.
  - The rule specifically exempts these disclosures from the BAA treatment.
  - Health care providers often disregard the exemption and request a BAA even though one is not required.

Key Steps for Achieving HIPAA Compliance

- Develop, adopt and implement privacy and security policies and procedures.
  - Adopt strict policies regarding the use of electronic mail. Ensure that any PHI that is transmitted outside of your internal network is encrypted.
  - Adopt strict policies regarding the storage of PHI on portable electronic devices (require encryption) and strictly regulate the removal of any portable electronic devices containing PHI from the premises.
- Appoint a privacy officer and a security official

Key Steps for Achieving HIPAA Compliance

(cont'd.)

- Conduct a risk assessment to identify vulnerabilities to the confidentiality, integrity and accessibility of PHI under the direction of the security officer. Remediate any risks and revise policies as appropriate.

- Map the flow of PHI throughout your organization and identify (i) all places where PHI is stored; and (ii) all individuals who access PHI.

- Train all employees who use or disclose PHI and document employee participation in training. Conduct refresher training on an annual basis.

Key Steps for Achieving HIPAA Compliance

(cont'd.)

- Publish and distribute a Notice of Privacy Practices: distribute to patients, obtain acknowledgment of receipt, display on the company's webpage and update when policies are revised.

- Enter into valid, HITECH Act compliant business associate agreements with all business associates and subcontractors.

- Adopt and implement a protocol for investigating potential breaches of PHI, documenting the results of the investigation and achieving the requisite notifications in the event of a breach.

Key Steps for Achieving HIPAA Compliance

(cont'd.)

- Sanction employees appropriately in the event of a violation.

- Monitor program implementation on an ongoing basis.

Breach Notification Obligations – Post-HITECH Act

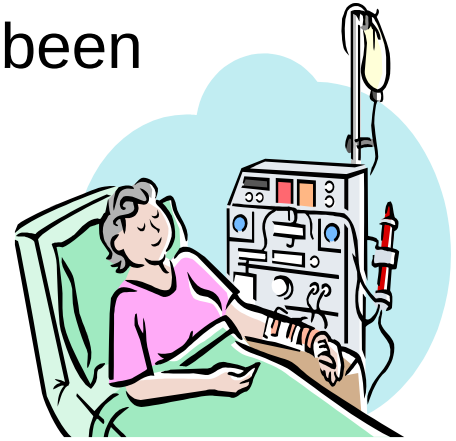
- Responding to a Potential Breach
  - Covered entities must notify affected individuals when a breach of unsecured PHI occurs or is reasonably believed to have occurred
    - Breach is the unauthorized acquisition, access, use, or disclosure of unsecured PHI which compromises the security or privacy of such information
    - Unsecured PHI has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals by HHS approved methods
  - Harm threshold – Covered entities must determine whether the use or disclosure poses a significant risk of financial, reputational, or other harm to affected individuals?

Breach Notification Obligations *(cont'd.)*

- Examples of Potential Breach
  - Patient information mailed or faxed to wrong patient or other recipient
  - Patient record accidently left in a public place
  - Patient financial information transmitted for reimbursement is intercepted by a third party or lost in the mail

Example

A dialysis patient crashes in the unit and must be rushed to the hospital. The facility administrator attempts to fax the patient's records to the hospital but inadvertently sends them to a local television station. The patient is a former professional basketball player for the local team and his medical records indicate that he has recently been diagnosed with HIV/AIDS.

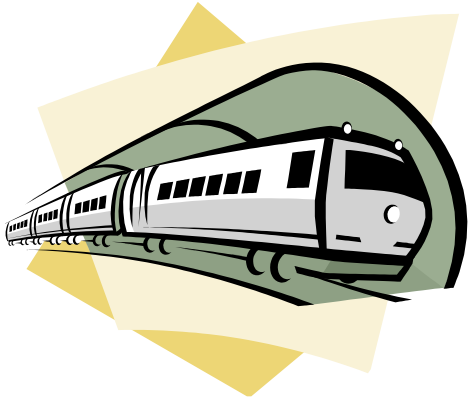


HIPAA Enforcement

Mass General – "The Million Dollar Subway Ride," February 14, 2011

- An employee of General Hospital Corporation and Massachusetts General Physicians Organization Inc. left documents on a subway that included a patient schedule containing PHI of 192 patients, and billing forms with PHI for 66 of those patients. The billing forms indicated a diagnosis of HIV/AIDS for certain patients.

  - The HIPAA Privacy Rule requires health plans, health care clearinghouses and most health care providers (covered entities) to protect the privacy of PHI through administrative, physical and technical safeguards at all times.



Mass General – "The Million Dollar Subway Ride," February 14, 2011

- Mass General paid the US Government a $1,000,000 settlement and entered into a Corrective Action Plan ("CAP"):
  - Develop and implement policies and procedures that ensure that PHI is protected when removed from Mass General's premises;
  - Train workforce members on these policies and procedures; and
  - Designate the Director of Internal Audit Services to serve as an internal monitor who will conduct assessments for compliance with the CAP and render semi-annual reports to HHS for a 3-year period.

April 17, 2012 – Phoenix Cardiac Surgery, P.C.

- PCS posted clinical and surgical appointments for patients in an on-line calendar that was publicly accessible
- Practice also failed to comply with numerous HIPAA requirements
- HHS Office for Civil Rights imposed a fine of $100,000 and enter into a one-year corrective action plan

Increased Civil Penalties and Expanded Criminal Liability for Violations – Covered Entities and BAs

- The maximum civil penalty for uncorrected willful neglect increased from $25,000 to $1,500,000

- Civil and criminal liability extends to Business Associates

Mandatory Compliance Audits

The Secretary of HHS is required to perform periodic compliance audits of covered entities and Business Associates

B. State Privacy Laws and Circumstances That Extend Beyond HIPAA Requirements

III. Legal Implications or Other Transitional Circumstances

A. Patient Abandonment

- State Law Requirements

B. Patient Discharge

- Conditions For Coverage For ESRD Facilities

III. Legal Implications or Other Transitional Circumstances *(cont'd.)*

C. Patient Solicitation

- By Contract
- By State Law

“Quality is not an act. It is a habit.”

~Aristotle

The End

41928405.1.ppt.