From: Mills, G. Foster
Sent: Tuesday, October 28, 2008 12:50 PM
To: *ALL EXCHANGE USERS
Subject: HIPAA Protocol for Safeguarding Medical Records
Attachments: 644584_2.DOC

Attached is a copy of the Law Department's protocol for safeguarding medical records pursuant to the Health Care Portability and Accountability Act (HIPAA). Please read it carefully and follow its instructions when dealing with the documents and materials it discusses. If you have any questions about the protocol, please contact your division's HIPAA coordinator, or Martha Mann Alfaro at 212-788-1084 or malfaro@law.nyc.gov.

The protocol can also be found in the Useful Links list on the Law Department intranet home page and in the office manual under Standards of Conduct.

Thank you.

LAW DEPARTMENT PROTOCOLS FOR SAFEGUARDING MEDICAL RECORDS

The "HIPAA Privacy Rule," issued by the U.S. Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act, affects how we handle some of the medical information that comes through our offices as we represent our clients. However, we believe that the safeguards required by the federal rules are appropriate for all the medical information we handle. Therefore, the Law Department has adopted the following protocols for information that describes a person's past, present or future mental or physical health, the medical care provided to any person, and the payment for any such care. This protocol applies to all forms of communication about such information: oral, written, and electronic. Each division is to designate a manager responsible for enforcing these protocols. Employees who violate them will be subject to discipline.

I. GENERAL SAFEGUARDS

Treat all medical records as confidential. Do not disclose information in the records to anyone except as necessary to represent our clients.

When requesting medical information from clients, ask for the minimum necessary to perform your task. In some circumstances, an entire medical file may be the "minimum necessary." If you request an entire medical record from one of our clients which is a "covered entity" you will need to represent that the information is the minimum necessary for the purpose of carrying out the legal representation of the client.

Do not discuss anyone's medical history, medical claims, or medical records in public places, such as hallways, elevators, or the cafeteria.

Do not discuss a plaintiff's or witness' medical records or condition on the phone when people are present in your office who are not involved with the case..

When carrying medical records around the office, put them in a file folder or a red weld.

When someone you don't know asks you for medical information about a witness or plaintiff, do not disclose the information until you have taken steps to verify that person's identity and authority to ask for the information. Find out where the person works, what is their position, and what is their basis for needing the information. Disclose only the information they need to know. If you have doubts about whether it is appropriate to disclose information to them, consult your supervisor. If reasonable under the circumstances, you may rely on the following to verify the identity of a person requesting medical information:

- The request is made in person by someone with a government identification badge or other official credentials, or other proof of government status, such as a written statement on government letterhead.

- The request is made in person by someone acting on behalf of government, and the person has evidence of this such as a contract for services, memorandum of understanding or purchase order.

- The request is made in writing on government letterhead.

If reasonable under the circumstances, you may rely on the following to verify a person's authority to request medical information:

- A written statement of the legal authority, or an oral statement when the written statement would be impracticable.

- The request is made pursuant to legal process, warrant, subpoena, order, or other process issued by a grand jury or a judicial or administrative tribunal.

II. PHYSICAL PLANT

A. PERIMETER SECURITY

Be very careful about allowing people you don't know into the office areas, especially in those offices that do not have lobby security at the present time. While it might seem rude, do not hold the entry doors open for anyone following you in.

B. FILES

At the end of a work day, put the contents of a file in a redweld and return the file to the file room or in a lateral cabinet in your office or on/under your work station desk.

If you are working on medical files, turn them over when you leave your desk and when other people visit your office or work station.

Whenever practicable, file cabinets and offices with medical records in them should be locked when not in active use.

C. FACSIMILES

Use a cover sheet to transmit medical records when sending a fax. Do not include a message on the cover sheet that comments on the contents of the medical records. Include a confidentiality notice on the cover sheet. Inform those who are sending you faxes to follow these procedures.

In order to insure prompt receipt, call the recipient about the incoming fax.

Make sure the confirmation shows that the fax went to the correct location.

For delivery of incoming faxes, the HIPAA coordinator in each division will assign someone to regularly check the division fax machines.

If you have access to desktop faxing, use that method rather than regular faxing.

D. COPYING

If you copy some or all of a medical record in error, tear it up or, if a shredder is available, shred it. If you copy medical records, be careful not to leave originals or copies behind.

E. E-MAILS

When sending an e-mail containing medical information there should be a confidentiality notice on the e-mail.

F. PCs & LAPTOPS

Where practicable, computer monitors and laptops should be positioned so that they are not visible to persons passing by your desk or visiting your office. If this is not feasible, be sure to close or minimize any document that contains medical information when it is not in use.

III. LITIGATION

A. TAKING FILES HOME

If you take a file home, do not leave it where people can see the contents of the medical records.

B. TAKING LAPTOPS HOME

You can take your laptop, which has password security, home in order to complete work on abstracts, motions, etc. that discuss a plaintiff's medical records. Do not work in an area where others can see your screen.

C. E-MAILING DOCUMENT TO YOUR HOME COMPUTER

This is a problem if other people have access to your home computer. When working at home, you should protect any document that contains medical information about a plaintiff or any individual. There are a number of options available: (1) If your home operating system permits each user to have a password, then use your password to protect your work, (2) Send the document home as an e-mail attachment. Before sending the document, you can protect the document by giving it a password on your office pc. In Word, go to Tools, Options, the Save Tab, to File Sharing Options, type your password, save the changes, and send it to your home computer as a e-mail attachment.

(CAUTION: if you forget the password, the document cannot be retrieved so use a password you will not forget.) When you complete your work at home, send it via e-mail to work where you can then remove the password and save the changes. (3) You can work on a disc at home, but be aware that discs are vulnerable to crashing. (4) If you have access to Citrix, use that from home rather than e-mailing. Citrix is password protected.

IV. SUBCONTRACTORS

PRIVATE INVESTIGATORS – As a "business associate" of "covered entities," regulated by the HIPAA Privacy Rule, we require that our subcontractors, enter into an agreement that will maintain the restrictions and conditions of the Law Department's agreement with the covered entities.

MEDICAL RECORDS RETRIEVAL COMPANIES – Like private investigators, these companies must agree to comply with the standards for disclosure pursuant to their contracts with us.

V. HIPAA COORDINATORS

Each division shall appoint a coordinator to ensure the division's compliance with these guidelines and the provisions of HIPAA.