Teaching Physician Compliance ALERT

Published by the Yale Medical Group

September 2012 Issue 85

The main focus of the September edition of the Alert newsletter is on privacy issues stemming from the Health Insurance Portability and Accountability Act (HIPAA). Angela Oren, JD, is the Yale School of Medicine's senior deputy privacy officer and risk management administrator and the author of the HIPAA articles. Angela can be contacted at Angela.Oren@yale.edu or 203-737-1781.

FAIR WARNING: THE AUDITS ARE COMING

The HIPAA regulations include a little-known mandate to monitor access to patient information in electronic form, to the extent practicable. All of the systems that are currently in use can track who opened what record. Most cannot tell, however, how long a user was in a record, what screens were displayed, or whether any part of the record was printed.

With the Epic implementation, comes a dramatic advance in the ability to audit user activity. Not only will it be possible to know who does what, with the help of a program called "Fair Warning," it will be possible to glean information about the relationship between the user and the patient. For example, by drawing on data from Human Resources systems, Fair Warning will generate a report every time someone calls up the record of a coworker, household member, or even a neighbor.

This is a monumental change. Until now, most audits have been conducted because of patients' complaints. People who browsed records with no work-related need to know, essentially gambled on not getting caught. And because of the sheer volume of transactions, the odds were in their favor.

But with Fair Warning, every transaction will be audited, and everything that looks like inappropriate access will be flagged for follow-up. Thus, even relatively benign uses of the data in Epic – for example, to find a colleague's home address, to send a gift – will be detected and will be subject to sanctions. These audits change cultures in ways that laws and regulations alone never could.

That said, HIPAA compliance should not disrupt anyone's normal activities, such as clinical care, medical education, billing, or administrative functions. If your job requires you to access or use a neighbor's protected health information, then you should do so, without hesitation.

However, if you choose to browse a friend's record – as opposed to having it assigned – you are violating University and YSM policy. Access, in the absence of a role-based need to know will bring sanctions, up to and including termination of employment or affiliation.

For further information about the audits or investigations, call Angela Oren at 203.737.1781 or e-mail ymg.privacy@yale.edu.

HOW TO CHOOSE HIPAA STRONG PASSWORDS THAT YOU CAN ACTUALLY REMEMBER

Online passwords are a non-negotiable fact of life. Everybody has at least one. Many of us have a dozen or more passwords for the programs we access, the websites that we regularly visit, or even just to use our computers.

Because passwords hold the key to valuable information, hackers and identity thieves work around the clock and world trying to guess what they are. As guardians of the privacy of patient information, an important part of our job is to make their job more difficult. Computer security experts recommend avoiding obvious choices for passwords – such as usernames, users' birthdate, words that can be found in the dictionary, and names of relatives. Another best practice is to use a mix of letters – upper and lowercase – and numbers, as well as symbols if possible. The result of such a password, is by definition somewhat meaningless, and therefore difficult to remember; something like wPSb5s2!y, or g$KEpCo4.

Experts also advise against writing down these complex passwords. They liken it to leaving the key in the ignition of your car. Rather, they recommend finding a way to give meaning to your password, so that you will be more likely to remember it.

One way to do that is to use the initial letters of words in a favorite poem, phrase, quotation, or song lyric. Because the most secure passwords contain a combination of upper and lowercase letters, symbols, and numbers, the letter I could be represented by the number one, the letter O by zero, the letter T by a plus sign, lower case L to I, etc. Thus, the first line of the song, Twinkle, Twinkle Little Star ("Twinkle, twinkle, little star, How I wonder what you are") could be made into a strong password as follows:

The initial letters, all alphabetical, and all capitalized would yield: TTLSHIWWYA

Changing some of the capital letters to lower case, and others to symbols would result in something like: ++LSH1WWYa

- Strive for consistency in how you substitute numbers or symbols for letters. You will end up creating a kind of password alphabet that will quickly become familiar.
- If you choose a short phrase, you can write the whole thing, in one word, using your coded alphabet. For example, $EREn1tyNow! pLAy1+Aga1nsam or ltl$WhatITI$.
- Avoid using your name, and the names of your relatives, or any other words or dates that would be obvious choices to anyone who knows you.
- Choose a different password for every site or application that creates, uses, or stores Protected Health Information.
- Consider using a different theme for each site or application that you use. For example, fictional characters for Epic, sports teams for your Net ID, and song lyrics for online shopping.

HIPAA HORROR STORIES

Stanford

In October 2011, the names and diagnosis codes of approximately 20,000 patients of Stanford University hospitals were found posted on "Student of Fortune," a website that offers students help with homework. Stanford's investigation revealed that a consultant, who had received the data as part of an engagement, had given it to an applicant as part of a practical job interview process. When the applicant turned to Student of Fortune for help in completing the assignment, s/he uploaded the patient information to their website. At the conclusion of the Department of Health and Human Services (DHHS) Office of Civil Rights' (OCR's) investigation, the contractor might be subject to fines of as much as $1,500,000. A number of patients have already filed suit against Stanford Hospital, seeking a collective settlement of $20,000,000, under California's medical record privacy law. In addition, Stanford's "Business Associate" might be liable for damages if any of the patients prevail in civil suits.

M.D. Anderson

In June 2012, an unencrypted laptop computer containing Protected Health Information belonging to 30,000 patients was stolen from the home of a physician-researcher at M.D. Anderson Cancer Center. The data included medical record numbers, patient names, social security numbers, and clinical information. It included records going back more than ten years. No announcement has yet been made regarding fines or other penalties. However, depending on the results of the investigation of the primary HIPAA enforcement agency, the DHHS OCR, and the timing and circumstances of the data collection, fines might range from $300,000 to $4,000,000; not including damages from civil suits, if any, if patients were harmed as a result of the incident.

Memorial Sloan-Kettering

In June 2012, a PowerPoint presentation containing Protected Health Information was discovered to have been posted, for more than five years, on the Internet. The presentation, which was intended for use by members of two professional medical organizations, was created by Memorial Sloan-Kettering staff. The presentations could be located through searches of patients' names. However, the patient information was obscured by graphs and other illustrations, and was therefore visible only if the images were manipulated; e.g., by downloading and enlarging them. No penalties have yet been announced. However, OCR might impose fines of $100 to $50,000 for each record posted. Additional penalties, including civil damages, might also apply.

St. Louis Plastic Surgery Practice

In August 2012, a St. Louis plastic surgeon posted before-and-after photographs of thirty women who had undergone breast augmentation, on her website. Though their faces were obscured, the patients sued for negligence when they discovered that the pictures included identifying information, and that the site could be located simply by searching for the patients' names. Ten of the patients have filed suit for invasion of privacy, seeking unspecified damages. OCR's investigation is still pending.

E&M MEDICARE AUDITS

Our Medicare contractor, National Government Services (NGS), is conducting service-specific prepayment audits on the following current procedural terminology (CPT) codes, billed by Connecticut Medicare Part B providers in the subsequent specialties:

* 99223 - Initial hospital care, per day, for the Evaluation and Management (E&M) of a patient billed by general surgery physicians;

* 99233 - Subsequent hospital care, per day, for the E&M of a patient billed by cardiologists and gastroenterology physicians; and,

* 99215 - Office or other outpatient visit for the E&M of an established patient billed by hematology/oncology physicians.

Each of these CPT codes is associated with high medical decision making (MDM). There are three areas to consider when judging the level of MDM.

1. How many diagnoses or management options are you dealing with? If the patient presents with a problem that is new to you or an established problem that is worsening, your level of MDM will be higher.

2. What is the amount and complexity of the data involved in the visit? Reviewing and/or ordering diagnostic studies adds to the complexity of the MDM. Independent review of images or reviewing old or transferred medical records also adds to the complexity of MDM and should be clearly documented in the medical record.

3. What is the overall risk to the patient? If the presenting problem(s) fall into any of the following categories, the level of MDM is high:
   - One or more chronic illness with severe exacerbation;
   - Progression or side effects from treatment;
   - Acute or chronic illnesses or injuries that may pose a threat to life or bodily function; and,
   - Drug therapy requiring intensive monitoring for toxicity.

The level of MDM is determined by looking at all three of the above criteria. Conditions that may meet high MDM would include multiple trauma, acute MI, pulmonary embolus, severe respiratory distress, progressive, and severe rheumatoid arthritis, and psychiatric illness with potential threat to self or others.

IN THE NEWS

Wallingford Man gets 7 years for prescription narcotics scheme

Jonathan Cosgrove, 27, of Wallingford, was sentenced in August to 84 months of imprisonment, followed by three years of supervised release, for conspiring to obtain and distribute oxycodone through the use of fraudulent prescriptions. On March 22, 2012, a jury found Cosgrove guilty of one count of conspiracy to possess with the intent to distribute oxycodone.

According to the evidence at trial, between August and November 2010, Cosgrove conspired with Raymond Zona and William Fabrizio to pass 18 fraudulent prescriptions, each for 180 oxycodone pills, at a Walgreens in North Haven. Fabrizio, who was employed as a pharmacy technician at the store, received between $150 and $250 from Cosgrove and Zona each time he filled a fraudulent prescription. Cosgrove and Zona would use some of the oxycodone and sell some of the pills to others for profit.

Cosgrove's criminal history includes previous convictions for passing fraudulent prescriptions.

Zona and Fabrizio each pleaded guilty to one count of conspiracy to possess with the intent to distribute oxycodone. On July 13, 2012, Zona was sentenced to six months of imprisonment. On August 1, 2012, Fabrizio was sentenced to three years of probation, the first six months of which he must spend in home confinement with electronic monitoring.

In October 2010, the U.S. Attorney's Office and members of federal, state, and local law enforcement, and regulatory agencies initiated "Operation Pharm Team" to combat the misuse of prescription drugs. According to David B. Fein, United States Attorney for the District of Connecticut, "The illegal distribution of prescription narcotics is a serious and rising problem in Connecticut and nationally. … May this sentence serve as a warning to those involved in the illegal distribution of prescription drugs: You will be prosecuted and sentenced like other drug dealers." Source: U.S. Attorney's Office

Illegally dispensed prescriptions gets pharmacist sentenced

Daniel Fiore, 60, of Brooklyn, was sentenced September 6, 2012 to two years of probation and a fine of $20,000 for unlawfully dispensing controlled substances. Fiore must serve the first six months of his probation in home confinement under electronic monitoring by the United States Probation Office.

According to court documents and statements made in court, Fiore owned and operated Daniel's Pharmacy, a retail pharmacy located at 42 Reynolds Street in Danielson. In 2009 and 2010, Fiore unlawfully dispensed a Schedule III controlled substance containing a mixture of hydrocodone and acetaminophen (generic Vicodin) and Schedule IV controlled substances, including diazepam (Valium), alprazolam (Xanax), or triazolam (Halcion) to friends and family members without any valid prescriptions for such medications. In order to conceal his conduct, Fiore created fraudulent prescriptions in his own handwriting, as if the prescriptions had been called in by a physician's office, and then documented filling the prescriptions in the same manner that he documented legitimate prescriptions. In total, Fiore unlawfully dispensed 1,542 tablets of Schedule III and 210 tablets of Schedule IV controlled substances.

Fiore agreed to surrender his federal and state licenses to dispense controlled substances after his arrest. Source: U.S. Attorney's Office.

Teaching Physician Compliance ALERT

Published by the Yale Medical Group

Compliance Programs—Preventative
Medicine for Healthcare Providers

P.O. Box 9805
New Haven, CT 06536
1 (877) 360-YALE hotline
http://comply.yale.edu/medicalbilling

Chief Medical Officer: Ronald Vender, MD
Compliance Medical Director Joshua Copel, MD
Director of Medical Billing Compliance: Judy L. Harris
judy.harris@yale.edu | (203) 785-3868