

# Prying Eyes

## Protecting Your Personal Health Information

By Randi Kopf, R.N., M.S., J.D.  
Kopf HealthLaw, LLC



© Copyright 2007, Stephen Mcsweeney—Agency: Dreamstime.com

Is your personal health information (PHI) more private since the implementation of the Health Insurance Portability and Accountability Act of 1996<sup>1</sup> (HIPAA) Privacy<sup>2</sup> and Security<sup>3</sup> laws? Is it possible that your PHI can be exposed to more prying eyes than before?

How would you react if you went to a doctor who specialized in Alzheimer's disease, and you used your employment health plan for the visit, and then a few days later you find out that your test results were faxed to your office and viewed by a co-worker who mentioned the faxed test information to others in the office while trying to locate you?

Patients with fibromyalgia have a special interest in maintaining the privacy of their personal health information. Currently it is known that PHI has influenced employment decisions including hiring, premature terminations and promotions as well as pricing and coverage determinations for insurance policies including health, disability, and life insurance coverage. PHI even affects school placements for young people.

Incorrect perceptions about a medical condition also impact social interactions. For example, your name is removed from the list of chairpersons for your neighborhood event after you mentioned to the organizer that you couldn't attend meetings on Tuesday because that is your PT day. In another instance, when a lawyer's colleagues learned of her diagnosis, they assumed she could no longer handle client referrals. Fortunately, one colleague asked her if she "felt up to" a new case, and the incorrect perception was remedied, at least for that one colleague.

The general public as well as many health care professionals still do not understand the nature of fibromyalgia, or worse, assume it includes an inability

to work or participate, a permanent disability, or a psychosomatic disorder. As the National Fibromyalgia Partnership continues to educate the public and professionals, these incorrect associations will diminish.

Every time you go to a new doctor, hospital, or health care facility or pick up a prescription at your local pharmacy, what are you asked to sign? The following is a brief overview of the privacy aspects of HIPAA, the first national privacy regulations.

**What do the HIPAA Privacy laws require of all health care providers (all health care professionals, hospitals, laboratories and any place that provides health care services or retains PHI)? Providers are required to:**

- ❖ Create privacy practices, policies, and plans in accordance with federal and state published guidelines and law
- ❖ Write and make easily accessible a *Notice of Privacy Practices* (NPP) that includes:
  - ◆ A statement that their professionals, employees, business, third party contractors or suppliers have a legal duty to keep your personal health information confidential and are committed to be in compliance with all federal, state and local law and regulations.
  - ◆ The Notice should also include the provider's general privacy policies
  - ◆ What steps the provider takes to ensure privacy
  - ◆ How and when the provider is permitted to disclose your PHI

◆ Your rights pertaining as a patient under HIPAA and state laws:

- The right to request restrictions on uses and disclosures of your PHI. However, the law states that your provider may deny your request. A denial could occur if your physician thinks that your requested restriction may interfere with the medical care you need.
- The right to designate your preferred method of communication by the health care provider. For example, do not fax or email me at work; call me only at this number
- The right to read and obtain a copy your medical records (PHI)
- The right to request amendment or additions to your PHI
- The right to see a listing of where your PHI was disclosed
- You are entitled to a copy of the NPP
- How and where to file a complaint about the provider's privacy practices or if you believe that your PHI was disclosed inappropriately

❖ Health care providers are also required to obtain a written acknowledgment that the patient has read and understood the NPP. This is generally what the doctor's offices, pharmacies, hospitals and laboratories ask you to sign. If you are concerned about the disclosure of your PHI, be sure to carefully read the information in the form and take advantage of your patient rights as needed.

❖ Health care providers are required to obtain written consent for certain disclosures of your PHI under HIPAA and often state law as well.

### **What are the HIPAA Security Rules?**

The HIPAA Security Rules direct health care providers to:

- ❖ Create policies regarding the security, use of and access to patients' electronic PHI
- ❖ Take reasonable steps to secure access to PHI stored on electronic media, such as computers, back up devices, imaging equipment (x-rays and Dexa scans) and handheld computer devices (PDA)

### **When are health care providers permitted to disclose your personal health information without your consent under HIPAA?**

- ❖ For treatment purposes, such as to another treating physician
- ❖ For payment purposes, such as to your health insurance plan
- ❖ For health care operations, such as calling you to remind you of an appointment
- ❖ When you need emergency health care services
- ❖ If the information is needed for law enforcement purposes
- ❖ If requested by lawful legal demand (such as a subpoena or request made by a court of law)
- ❖ If you have authorized the disclosure to another party, such as workers compensation or your lawyer

HIPAA is a complex set of rules, regulations and interpretations. The above information is only a small part of the law commonly referred to as HIPAA. Doctors, nurses and hospitals have always had professional responsibility to protect patients' privacy and the confidentiality of their PHI. HIPAA, in many ways, is the codification of this professional duty.

Each new expansion of computers into health care settings, for submission and payment of health care insurance claims and electronic medical records, exponentially increases the risk of inappropriate exposure of your PHI. The ease and speed of sending electronic information can mean in a click that your PHI may be sent to the wrong address on a computer screen. It could be seen by many co-workers in your office or be captured by cyber pirates for commercial sale. Your PHI has great commercial value, for example, to those who want to sell you health care related products. Another problematic disclosure would be the sending of your PHI to a bank which is considering your loan application. These are not hypothetical situations. In 2002, the pharmaceutical company Eli Lilly was charged by the FTC for disclosing online the names and phone numbers of 669 participants who were enrolled in an online reminder service for the antidepressant Prozac<sup>4</sup>.

## What can you do to protect your PHI?

❖ Carefully read any information or forms you are asked to sign or give consent

❖ If you have concerns about the disclosure of your PHI, or certain aspects of your PHI, such as references to alcohol rehabilitation, it is critical that you discuss these concerns with your health care provider. In addition, there are state and federal laws that protect certain PHI from disclosure without your specific written consent. Your health care provider is your advocate and the protector of your PHI. If there are specific persons or entities to whom you do not want your PHI disclosed, write this information very clearly on your patient information form and ask your provider to sign his/her acceptance of the request. Remember that only if your health care provider agrees not to disclose your PHI to that person or has not already sent your PHI prior to your request will your PHI not be disclosed. If your request is denied, you are entitled to an explanation in writing for the denial.

❖ Whenever you are asked to sign a consent form and there is something in it that you do not want to occur, such as photographing your surgery, cross through the words with one line and write your initials at the end of line to indicate you made the changes.

❖ When signing consent for disclosure, limit the amount of time the consent is valid. For example, you may permit disclosure of your information for one year only. It is not permissible for a provider to request that you sign a consent that lasts indefinitely.



© Copyright 2007, Jupiter Images

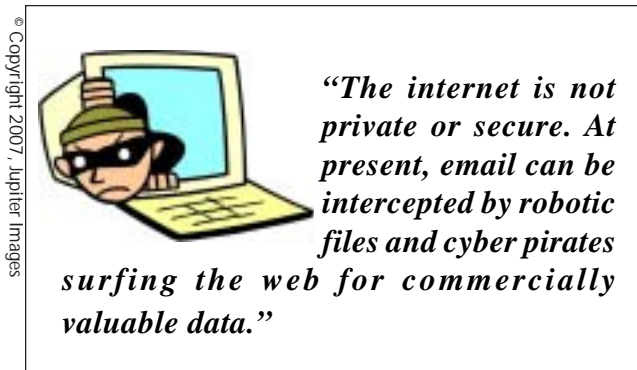
❖ You can revoke your consent for disclosure, but you must do so in writing and before the PHI is disclosed.

❖ Do not email your health care providers or accept emailed PHI information. At the current time, there is very limited confidentially secured email communication. The internet is not private or secure. At present, email can be intercepted by robotic files or cyber pirates surfing the web for commercially valuable data.

One of my clients called because a patient was irate that she was being solicited by a diabetic supplies company and wanted to know who in the doctor's office had released this information. It was determined that when the health insurance claim was submitted over the internet, the information was intercepted. Since the implementation of HIPAA, this is less likely to occur today.

Nevertheless, computer programmers continually develop multiple methods of intercepting information sent over the internet. Therefore, before you give consent to your health care provider to keep your PHI in electronic format or email you with lab results, etc., read the consent for electronic communications carefully, review the provider's privacy and security practices information, and make the terms of the PHI disclosure limited both in scope and time details.

As the use of electronic media and technology in health care becomes the customary practice, patients will have less and less ability to limit how and to whom their PHI is disclosed. But until then, take whatever steps you can to protect your personal health information.



© Copyright 2007, Jupiter Images

## References

<sup>1</sup> 45 CFR Part 160, 162

<sup>2</sup> 76 FR 53182, 45 CFR Parts 160 through 164

<sup>3</sup> 68 FR 8334

<sup>4</sup> *In the Matter of Eli Lilly and Company*, File No. 012 3214, Docket No. C-4047

**Randi Kopf, R.N., M.S., J.D.**, is a practicing health lawyer and former family/oncology nurse practitioner with her own firm, Kopf HealthLaw, LLC, in Rockville, Maryland. She serves as general and health counsel for individual physicians, medical groups, national and regional medical and allied health associations, health care practitioners and entities locally and across the country. She also represents certain individuals with health insurance matters. She is an invited member of the Maryland Attorney Grievance Commission and has served on the Maryland Health Care Commission EDI/HIPAA task force that developed nationally accepted privacy guideline tools. She currently serves on the Board of Directors of The American Association of Nurse Attorneys (TAANA).

Ms. Kopf has provided legal support for several U.S. Congressional health care bills and advocated on behalf of physicians before the US Attorney's Health Care Fraud Task Force. She has been a sought after speaker for national and state conferences on medical legal topics. Ms. Kopf has extensive teaching experience and has held instructor and faculty positions at Georgetown University, the University of Maryland, and Adelphi University. Her published work is also extensive.

Ms. Kopf is admitted to practice law in Maryland, DC, and the United States Supreme Court. Ms Kopf was Board certified as a Family Nurse Practitioner for over 25 years. She has received the Cornell University Alumni Award for Outstanding Volunteerism, the National Distinguished Service Award in Nursing, and the Distinguished Service Award for TAANA.

**Contact Randi Kopf at Kopf HealthLaw, LLC**

**Website: [www.kopfhealthlaw.com](http://www.kopfhealthlaw.com)**

**Direct dial: (301) 251-2788**

