

Information Security Protections for the Consumer

by Angela K. Dihn, MHA, RHIA, CHPS

Over the past several decades, the evolution of technology has changed the practice of medicine and will continue to do so. With these technological advancements come an increased risk to the consumer. Consumers must be made aware of the risks, the available protections, and the proactive steps that can be taken against these risks.

Two of the biggest risks in health information include data breaches and medical identity theft. Data breaches happen every day and in many different ways. A data breach can range from the actual hacking of information (for example, a computer) and data theft, to the loss of portable devices and more. Medical identity theft is one of the fastest-growing information crimes in America. It can be the result of stolen information, like a social security number, or insurance information used to falsify patient care for someone other than the individual, and more.

As a consumer, you should be aware there are federal regulations that help protect you from these risks. Some of these regulations include the Health Insurance Portability and Accountability Act (HIPAA), the “Red Flags Rule,” and the newly enacted American Recovery and Reinvestment Act (ARRA), each discussed briefly below.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA was originally enacted in 1996 for different purposes than it serves today. In April 2003, the HIPAA Privacy Rule became effective enforcing a higher level of confidentiality practices for your health information whether in paper or electronic format. The Privacy Rule also gives patients certain rights to their health information in regards to who can see it, how it is used, and who it can be shared with, among other safeguards. In April 2005, the HIPAA Security Rule became effective, complementing the Privacy Rule and mandating protections of all electronic health information both in transit and at rest. Together, the privacy and security rules work

together to keep your information safe and secure from health information risks.

The “Red Flags Rule”

A major federal initiative against medical identity theft is the Federal Trade Commission’s (FTC) “Red Flags Rule” due to be effective June 2010, though this date is subject to change. The rules mandate that any healthcare provider who extends credit to their customers to develop a program to guard against identity theft that identifies and detects the relevant warning signs or “red flags” of identity theft. These may include, for example, unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents¹.

American Recovery and Reinvestment Act (ARRA)

In February 2009, President Obama signed ARRA into law. One of the results of ARRA was strict regulations on processes to complete following a health information breach. After a breach of more than 500 people occurs, affected consumers must be notified immediately either by the media (for example, the Internet, newspapers) or directly by mail or e-mail with detailed information on ways to assist with consumer protection and processes, and any potential risks. For detailed information on ARRA and the breach notification regulations, visit www.ahima.org/arra

These are just a few of the many consumer protections available to you, but it is important that you educate yourself by speaking with your healthcare provider, reading and researching information, and learning what you can. Be aware of the risks and know what steps you can take to protect yourself. Be proactive!

1. Federal Trade Commission. “New ‘Red Flag’ Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft.” Available online at www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm.

Quiz

Test your understanding of medical identity theft and the healthcare industry’s efforts against it:

- 1. Which rule provides protection for electronic information both in transit and at rest?**
 - a. Red Flags Rule
 - b. HIPAA Privacy Rule
 - c. HIPAA Security Rule
 - d. ARRA Breach Notification Regulations
- 2. HIPAA was originally enacted in 1996.**
 - a. True
 - b. False
- 3. Which rule provides protection for all health information whether it’s in paper or electronic format?**
 - a. ARRA Breach Notification Regulations
 - b. Red Flag Rules
 - c. HIPAA Security Rule
 - d. HIPAA Privacy Rule
- 4. Following a breach of 500 or more people, an organization can notify the individuals using which method?**
 - a. Internet
 - b. E-mail
 - c. Newspaper
 - d. All of the above
- 5. The Red Flags Rule help protect against medical identity theft.**
 - a. True
 - b. False