

Medical Identity Theft Protection for the Consumer

by Beth Hjort, RHIA, CHPS

Identity theft is an increasing threat to US citizens. Media reports of compromised information security are commonplace, and real-life stories are often exchanged. Most consumers are more familiar with financial identity theft such as unauthorized credit card use, than medical identity theft (MIT), a subset but no less concerning healthcare reality. A consumer’s best defense then is being well versed in both.

Medical identity theft occurs when an individual’s health information is misrepresented and used by an unauthorized individual to obtain healthcare goods, services, or money to which they are neither eligible nor entitled. The MIT activity occurs in the name of, but unbeknownst to, the victim. The insidious nature of an occurrence can make it difficult to detect and reverse. It can result in creation of inappropriate medical record documentation, financial burden or exhaustion of insurance benefits to the victim, or worse: harmful healthcare decisions made on behalf of the victim, based on the perpetrator’s information.

Heightened concern over malicious and criminal behavior has inspired enactment of laws placing significant responsibility on business and industry for adequate security safeguards and mitigating actions when breaches occur. These include data breach notification laws, specifying that affected individuals must be alerted to information leakage. But despite the ongoing threat of identity theft, consumers haven’t stopped using and appreciating technology’s benefits. The system has become a way of life, so careful personal choices about information handling are a crucial aspect of the fight against MIT.

The effort to stay ahead of criminal activity is in place on many fronts in healthcare, but we aren’t there yet. It will take a concentrated and united effort to achieve this goal. The strength of security technologies and insight into criminal behavior will continue to grow and become more sophisticated. Yet even when incidents decrease, vigilance remains critical at every portal. Healthcare delivery organizations, health plans, and individual citizens have a formidable role in protecting health information. For the consumer who wants to start right away, there is help. He or she can choose a position of offense (implementing wise choices with information use and handling), and second, a position of preparedness for immediate action if an incident occurs. An MIT Response Checklist developed by AHIMA provides free response guidance for a consumer victim. To access the checklist, visit [here](#) or , visit www.myphr.com, click on the “Keep Your Health Information Safe” button, and scroll down to the “Medical Identity Theft Response Checklist” link.

You may notice you are asked to confirm more identifying information when you register for health services at your provider than in the past. A new federal law, known as the Red Flag Rule, initiates a protective plan that triggers investigative action when suspicious conditions suggest an identity theft may be underway. Just as conscientious retailers pause to check the validity of a credit card purchase, you may be prompted for more information. When this happens—especially after May 1, 2009—it’s all part of the provider’s steps to protect you from the dangers of identity theft.

QUIZ

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

- 1. Identity theft and medical identity theft (MIT) are synonymous, with cause and effect appearing the same in the impact on a victim.**
 - a. True
 - b. False
- 2. Medical identity theft can result in:**
 - a. Fraudulent use of insurance benefits
 - b. Falsified medical record entries
 - c. Compromise in patient care quality and safety
 - d. All of these
- 3. Responsibility to react and contain MIT incidents rests with which of the following sectors?**
 - a. Healthcare providers
 - b. Health plans
 - c. Consumers
 - d. All of these
- 4. Current efforts to protect the consumer from identity theft and medical identity theft include:**
 - a. Most states have passed data breach notification laws
 - b. Federal Trade Commission’s Red Flag Rules
 - c. Providers, health plans, and consumers development of front-end and back-end preparedness and mitigation plans
 - d. All of these
- 5. A consumer’s self-protective actions can influence the likelihood and degree of impact of a medical identity theft incident:**
 - a. True
 - b. False

Answers: 1. b, 2. d, 3. d, 4. d, 5. a