MEDDATA SERVICE BUREAU

MEDTRON SOFTWARE INTELLIGENCE

051415 NEWS BLAST

MEDICAL IDENTITY THEFT

Medical identity theft occurs when someone steals a patients personal information (name, Social Security number, or Medicare number) for the purpose of obtaining medical care, drug services, or to submit fake billings to Medicare in the patients name. Often the information is stolen by employees at medical facilities, and resold. But most of the time, the culprit is someone close to the victim. Data thieves also may hack into medical databases or break into medical facilities. Medical identity theft can not only cause issues for a practice but can disrupt a patient's life, damage their credit rating, and waste taxpayer dollars. The damage can also be life-threatening to the patient if wrong information ends up in the patient's personal medical records.

While identity theft is a global issue that garners much media attention, most do not realize that medical identity theft is a serious and growing threat. Many authorities consider medical identity theft one of the fastest growing crimes in America. With the digital age of healthcare upon us, the risks are expected to increase as electronic medical records become more prevalent and the exchange of this data over expanding networks becomes more pervasive. Heightened concern over personal data security and privacy highlight the importance of having secure electronic medical identities.

A recent article in the *St. Louis Business Journal* related to medical identity theft, states that medical identity theft is currently the fastest growing identity crime in the United States, and argue that although "medical identity theft is most harmful to a consumer, organizations that handle personal health information can suffer costly legal ramifications as well as a tarnished brand if they are the source of the data breach." In addition, a recent survey found that 48% of respondents said they would consider changing healthcare providers if their medical records were lost or stolen.

"The threat of medical identity theft has increased, in part, because of breaches, including the massive attack on Anthem Inc., one of the nation's largest health insurance companies. Hackers stole information on a reported 80 million Anthem customers and employees. Until recently, there wasn't a lot of data to steal from medical records because digitization is relatively new. The Anthem breach did not appear to involve credit card or medical information -- only names, birthdays, Social Security numbers, income and other personal data, the company said. Medical facilities and insurance companies often don't have systems in place to alert a patient to unusual activity, unlike banks, credit card companies and other financial institutions. Also, while a bank or credit card will usually refund a patients money or remove suspicious charges while an incident is investigated, a patient might immediately find themselves on the hook for a fraudulent medical bill." (Source: Bankrate.com, Medical identity theft: Why you should worry)

The American Recovery and Reinvestment Act (ARRA) and the associated provisions under the Health Information Technology for Economic and Clinical Health (HITECH) Act and the Health Insurance Portability and Accountability Act (HIPAA) have highlighted the need to address privacy and security across our healthcare system. In fact, HITECH requires that consumers be notified of healthcare data breaches. Alerting patients when their personal health information has been breached is a necessary response, but it is a reactive measure. It does nothing to prevent the breach or address the subsequent issues patients face when they are victims of medical identity theft. The healthcare industry also needs policy that takes a proactive approach–one that implements controls and technology that assure patient information is always protected.

The HIPAA Privacy Rule (http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html) establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients' rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

The HIPAA Security Rule (http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html) establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

The HIPAA Breach Notification Rule (http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html) requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.

Practices/Provides must educate themselves with these rules and others to confirm standard are being met and patient's medical records are safeguarded at all times. Penalties for not adhering to these rules can cost thousands of dollars for individuals and/or practices.

Resources:

HHS: http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html
St. Louis Business Journal: http://www.bizjournals.com/stlouis/blog/2015/03/medical-identity-theft-is-fastest-growing-identity.html
OIG Medical ID Theft / Fraud: https://oig.hhs.gov/fraud/medical-id-theft/
Federal Trade Commission: http://www.consumer.ftc.gov/articles/0171-medical-identity-theft
Coalition Against Insurance Fraud: http://www.insurancefraud.org/scam-alerts-medical-id-theft.htm
USA Today: http://www.usatoday.com/story/money/personalfinance/2014/09/13/identity-theft-hacking-medical/15345643/
NBC News: http://www.nbcnews.com/tech/security/stolen-identity-2-3-million-americans-suffer-medical-id-theft-n311006
Bankrate: http://www.bankrate.com/finance/insurance/medical-identity-theft.aspx
Smart Card Alliance: http://www.smartcardalliance.org/publications-medical-identity-theft-in-healthcare/

Contact Software Support for assistance or any questions via:

From **MED**PM or **MED**EHR Sign On screens, double click on 'support@medtronsoftware.com' to compose an email to the Software Support Dept.

-OR-

Phone: (985) 234-0599 (local)
(800) 978-0599 (toll free)

-OR-

Fax: (985) 234-0609