



Kurt Long

The Impact of EHRs and Medical Identity Theft on Patient Safety

Safeguarding patients' privacy is of the utmost importance as implementation of EHRs grows, but another matter, protecting patients' emotional and financial well-being in securing their medical records is an increasing concern.

By Kurt Long

The benefits of electronic health records are undeniable, and the implementation of EHRs in the United States and globally is inevitable. However, without the health care industry's immediate attention to guarding against widespread and growing health care information crime, the industry is poised for a setback.

Organized criminals, being risk-averse and efficient, have taken notice that health care providers have the same identity information as financial institutions, as well as the patient's health insurance information. So a new, insidious form of identity theft has emerged--medical identity theft.

In this version, the criminal obtains the health insurance information of the victim, almost always for the sake of financial gain. The medical identity of the victim is sold to a criminal or crime ring, and false claims, usually through Medicare, are made against the victim. Frequently, the criminal maximizes the insurance benefits of an entire family, demonstrating the efficiency of organized crime.

A Brewing Crime Wave

Slowly and quietly, the health care industry has become a major target of information crimes. In the past decade, the financial industry has been plagued by security incidents and harassed by watchdog groups, driving the industry's investment in more rigorous security systems and the enactment of federal and state laws.

Meanwhile, the health care industry has been lax in establishing stringent security protocols and processes largely due to the feeling that HIPAA provided all the protection needed. The fact that no government entity or watchdog agency is willing to put teeth into proactive information security auditing, enforcement and punitive follow-up further supports this attitude. Another argument perpetuating this lax approach was that there was no evidence of wide-scale privacy and information violations in health care.

The evidence, however, is available and compelling. Medical identity theft is occurring on a scale larger than anyone wants to admit. In 2006, the World Privacy Forum completed a comprehensive study of medical identity theft and estimated that 250,000 patients had become victims to date.

The Patient Safety Consequences

The patient safety implications of medical identity theft are far-reaching and include financial, emotional, professional and health damages to the victim-patients. Blood type, disease history, prescriptions and other permanent health information are often changed in the victim's records in the process of submitting false

This article first appeared on June 13, 2007 in HHN's Magazine online site.

To respond to this article, please click [here](#).

claims. These changes go unnoticed until medical insurance limits are maximized, a job is denied due to medical history or improper emergency care is rendered.

It is well-documented that there are insufficient laws and procedures for cleaning up medical records once they have been compromised. This also means the victim lives with the ongoing emotional strain from medical identity theft. Job loss, financial loss, physical risks and emotional suffering with little recourse are the true patient consequences.

Taking Action on EHRs

Enlightened health care providers recognize the benefits of EHRs and see an opportunity to differentiate themselves in competitive markets on the issue of safeguarding patient records.

Leading organizations committed to EHRs are holding themselves to the letter of the law with regard to HIPAA information security. This includes adhering to some of the more challenging sections, including:

- Implementing hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronically protected health information;
- Identifying and responding to suspected or known security incidents and mitigating, to the extent practicable, harmful effects of security incidents;
- Protecting against any reasonably anticipated uses or disclosures of protected health information; and
- Implementing procedures to regularly review systems activity such as audit logs.

As dry as these sections of HIPAA sound and as difficult to implement as they can be, they were designed to address the types of highly damaging incidents discussed here. And these regulations were developed specifically with patient care and safety in mind.

In the health care environment, particularly when including EHRs and RHIOs, auditing, protection and identification of threats to private information must be extended to include computer-to-computer transactions, not just the traditional person-to-computer transactions. This covers scenarios where automated record exchanges have been established across health care provider boundaries.

In addition to HIPAA-driven procedures, leading organizations are making themselves familiar with regulations such as the Sarbanes-Oxley Act and borrowing best information security and privacy practices from other industries, such as the financial services industry, which has become a model for third-party auditing processes for protecting against identity theft.

To implement these measures, enlightened health care organizations are taking a multi-pronged approach to stopping medical identity theft in their facilities. Other organizations would be wise to follow their lead.

Security and compliance culture: Striking the right cultural balance between employee trust and the seriousness of patient information safety and privacy can be trying. However, a health care provider must create a culture that holds patient information safety at the same level of importance as the physical care of the patient.

This article first appeared on June 13, 2007 in HHN's Magazine online site.

To respond to this article, please click [here](#).

Best practices: Virtually all health care organizations are facing the same kinds of challenges. Best practices have been established that every health care organization should be aware of and consider implementing. Vendors offer specialized information security and privacy auditing that leverage best practices accumulated from across the health care industry. These solutions can be thought of like anti-virus software that picks up signatures of the latest threats and periodically updates itself--in this case for privacy auditing and incident detection.

Admission processes: Before receiving treatment, patients should be required to present some form of picture identification. This has already helped reduce the incidence of the fraudulent use of insurance.

Information security monitoring: Medical identity theft thrives on open access to patient information to which health care organizations are susceptible. Solutions are now available that automate compliance and information security responsibilities relating to reviewing audit logs, identifying common incidents, streamlining incident investigations and mitigating damages when there is an incident. With the advent of these types of solutions, the interpretations of HIPAA regulations that cite implementation “to the extent practicable” may be broadened in the future.

Physical security: Never underestimate the aspect of physical security. Organizations must consider changing procedures or even the physical layout of a facility to protect patient information.

Proactive organizations are seeking information on the high-risk scenarios that present dangers to their patients' safety and their institutional viability. They deal with these scenarios head on, ensuring that they will not need to deal with them reactively later. The reactive approach is sure to set back EHRs wherever they are implemented. In this case, following the leaders makes sense for the health care industry.

Kurt Long is founder and CEO of EpicTide, a St. Petersburg, Fla.-based compliance and information security company.

GIVE US YOUR COMMENTS!

HHNMostWired welcomes your comment on this article. E-mail your comments to hhn@healthforum.com, fax them to *Most Wired Magazine* Editor at (312) 422-4500, or mail them to Editor, *Most Wired Magazine*, Health Forum, One North Franklin, Chicago, IL 60606.

If you would like a **FREE** Subscription to *Most Wired OnLine*, [please click](#) here to register.

This article first appeared on June 13, 2007 in HHN's Magazine online site.

To respond to this article, please click [here](#).