

The Grave Costs of Medical Identity Theft

The cost of medical identity theft in the U.S. is estimated at \$1 billion per year and growing. Estimations indicate that in a 1 year time span there were as many as 3.25 million victims of medical identity theft, and the impact is far reaching.

By Kurt Long

Posted on October 6, 2006

Consider this: The cost of medical identity theft in the U.S. is estimated at \$1 billion per year and growing. Estimations indicate that in a 1 year time span there were as many as 3.25 million victims of medical identity theft, and the impact is far reaching. It doesn't only impact the patient, but also the medical organizations that provide care. The extreme consequences of medical identity theft can threaten or take a victim's life and cripple a medical organization through lawsuits, damage to the organization's reputation and the consequences of HIPAA violations.

Over the last several years hundreds of health care providers across the U.S. and Canada have worked to improve their auditing, compliance and information security systems and procedures. During the process, security vendors have encountered innumerable anecdotes related to insider security incidents involving the privacy of patient information. Security vendors and medical organizations have learned never to underestimate human ingenuity in finding a way to open the proverbial locked door to private patient data.

Common health care incidents related to fraudulent access to protected health information fall into a few common categories with varying motivations ranging in severity from curiosity to criminal. Whatever the motivation, all unauthorized access to medical patient information is potentially illegal and in direct violation of federal and state laws.

Common Scenarios:

Internal users/employees reviewing the medical records of fellow employees

Internal users/employees reviewing their organization's executive medical records

Internal users/employees reviewing the medical records of a VIP

Self medical record examination

Internal users/employees reviewing the medical records of their relatives

Internal users/employees reviewing the medical records of their neighbors and outside friends and associates

Financial identity theft

The consequences of these common incidents include annoyance and distraction, financial loss, direct violation of federal and state law resulting in penalties, and of course, long-term institutional damage to an organization's reputation. At times the impact is severe as was the case with many recent well publicized security incidents, most notably the Veteran's Administration.

Health care providers always nod knowingly when this list of common information security risks is reviewed- and each provider brings their own anecdotes relating to the seriousness of these scenarios.

However, it has become obvious that the individual anecdotes we are hearing are contributing to an alarming trend in our industry-medical identity theft. Medical identity theft, according to the Federal Trade Commission grew by 197 percent from 2001 to 2005.

Deeper Reaching Trend

In May 2006, the World Privacy Forum released a report on medical identity theft detailing the trends and consequences of this fast growing phenomenon. Probably the most alarming statistic cited in the report is that according to the Federal Trade Commission, it is estimated that there were at least 200,000 instances of medical identity fraud.

With medical identity theft the victim literally loses possession of their "medical identity." A neighbor, a friend, a relative or a stranger takes on the persona of the victim. Often they use their medical insurance and receive medical care. A victim of medical identity theft can face grave consequences including financial loss, but there are more disturbing consequences that the victim may not discover for years. The victim may find false procedures in their medical records, changed medical records including blood type, false claims against their health insurance and maxed out health insurance policies for their entire family.

The crime of medical identity theft is driven by varying motivations and perpetrators. Organized crime is frequently involved and the perpetrators almost always collude with a health care provider's employees, associated physicians specialists or other insiders. When organized crime is involved, generally their goal is to rapidly submit false claims (often MediCare related) and receive payment quickly before moving on. Alternatively, as health insurance premiums have risen and riders have increased, the number of people desperate for health insurance coverage has increased. Medical identity theft is many times carried out by an individual who is desperate for health insurance and willing to take on the medical identity of their victim(s).

The criminal perception is that the policing and consequences of medical identity theft are lesser than traditional forms of crime such as drug trafficking or even traditional identity theft. Thus, while HIPAA has resulted in unquestionable improvements in patient privacy and security, it is time to ask more seriously how will HIPAA be enforced and what are the consequences for neglect?

Conditions That Breed Risk

Health care organizations by nature are collaborative. This culture of collaboration is well intentioned because it takes team work amongst a range of professionals to ensure proper patient treatment.

As health care organizations have grown, they streamlined and improved their processes through health care information systems (HIS) and a wide assortment of supporting applications, examples of which include: patient billing, electronic records management, radiology, pharmacy and automated drug dispensing, time and attendance and scheduling among a few.

In keeping the necessary spirit of collaboration, health care providers have granted electronic access to these applications to nurses, employees, physicians, specialists, supporting clinics and other partners.

Finally, as hospitals have merged together under competitive pressures, it brought together multiple hospitals each with their own collection of information systems. The result is a necessary "mish-mash" of mission critical systems that remain in operation and are being accessed from multiple geographic campuses and from a variety of off-site partners. Consolidation is time consuming and expensive, so most health systems have to live with this reality.

The result is that virtually all health care providers have an information system environment that is widely accessed by internal employees and external partners that is virtually impossible to audit and monitor for the prevalent security risks discussed here.

Minimize the Security Risks

What can health care organizations do to minimize security risks?

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

Best Practices: Virtually all health care organizations are facing the same challenges. There are best practices established that every health care organization should be aware of and consider implementing.

Admission processes: Require patients to present some form of picture identification before receiving treatment. For various reasons this can have challenges, but there are already examples of where this has helped reduce the incidences 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. There are solutions 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. In the past, these types of solutions were not available, today there are, and that may change the HIPAA interpretation that frequently cites that processes should be implemented "to the extent practice-able."

Physical security: Never underestimate the aspect of physical security. Organizations must consider changing procedures or even the physical layout of a facility to protect controlled access to protected health.

Know you organization's specific risks: Complete a risk assessment. Be aware of security risks that may be specific to your geographic location and specialty. For example it is well documented that medical identity theft and other forms of health care fraud are most prevalent in high growth communities.

HIPAA's Role in Patient Privacy

HIPAA was designed to protect patient privacy. Organizations grapple with how to ensure they are compliant. However, as a security vendor, one of the common questions customers ask is "are there any examples of where HIPAA has resulted in significant fine or penalty?" It appears this question derives from a genuine curiosity rather than an attempt to avoid responsibilities. To date, there have not been prominent examples where HIPAA was upheld and the neglectful faced significant consequences.

HIPAA has resulted in great strides in improving patient information safety and privacy, but in the interest of patient safety, it is time to ask what is next? What comes after the infamous HIPAA deadline? How will HIPAA be policed, are there real consequences for organizations that are neglectful in protecting their patients' information?

Closing Thoughts

In the end, organizations should do everything in their power to protect patient data, not because it is mandated by HIPAA, but because it creates a safer environment for patient care. Actively guarding against unauthorized access to patient data not only could potentially save a life, but it has great financial upside by deterring or defeating a threat that costs the industry an estimated \$1 billion a year.

Kurt Long is the CEO of EpicTide.