

Sarbanes Oxley : Technology : Survey

Identity Theft Survey Reveals Consumers are Concerned About Privacy and Protection

January 17, 2007 03:00 PM

Risk to Life and Health, Altered Medical Records and Loss of Confidentiality Rank Among Top Fears Related to Medical Identity Theft

A robust 98 percent of consumers believe that healthcare organizations have a responsibility to protect patient medical records however, only 40 percent of consumers feel confident that their healthcare providers are able to secure their medical records. This is according to a survey report released today by EpicTide, a leading provider of security solutions for the healthcare industry.

The survey commissioned by EpicTide and conducted by The Benchmarking Company, an independent research firm, measured consumer awareness of medical identity theft and patient safety concerns. The survey report explores issues including:

- Consumer awareness of medical identity theft and its consequences
- Rising rate of incidence of medical identity theft among the general population
- Consumers' understanding of their patient rights
- Consumer perceptions regarding the ability of healthcare organizations to protect patient records and ensure patient safety
- Consumer perceptions regarding the responsibility of healthcare organizations in protecting patient records and reporting security breaches.

The World Privacy Forum recently issued a report detailing the growing medical identity theft phenomenon that is estimated to have impacted 250,000 and theoretically as many as 3.25 million people. Victims of medical identity theft are often unaware of the



Kurt Long
CEO
EpicTide

crime and once discovered, left without recourse to correct their medical files or the financial implications of the crime.

Despite the growth of medical identity theft, the EpicTide survey results revealed that nearly half of consumers had never heard of medical identity theft. Consumers were largely unaware of the grave consequences associated with medical identity theft such as loss of life or risk to health, loss of confidentiality of medical records and financial hardship. However, when asked to rank which consequences of medical identity theft were of the most concern, potential risk to their life/health, the loss of privacy and confidentiality of their medical records and someone changing their medical records were top fears.

The survey illustrates consumers' belief that medical organizations have a legal responsibility to alert patients if someone has accessed medical records without the patient's consent, but only 51 percent of consumers think that healthcare providers know when someone has accessed patient records. Only 30 percent of respondents believe hospitals are diligent about informing potential victims of suspected breaches and unauthorized access to patient records.

"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 violating HIPAA regulations," said EpicTide CEO, Kurt Long. "The survey data reinforces EpicTide's belief that consumers expect medical organizations to 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 auditing and monitoring against unauthorized access to patient data can potentially prevent the medical, financial and emotional hardships that medical identity theft is causing for so many Americans."

To request a copy of the survey report, or to learn more about medical identity theft, please visit <http://www.epictide.com/documents/MIT-receive-more.html>. EpicTide offers custom demonstrations of its FairWarning 2.0 product, a highly flexible, scale-able solution for centralizing audit logs and addressing compliance and information security vulnerabilities.

For more information or to request FairWarning 2.0 product specifications, visit www.epictide.com

EpicTide is a leader in solutions that help organizations increase their security responsiveness, identify insider security incidents, automate compliance and reduce associated costs. The company is privately held and is located in St. Petersburg, Florida.

To learn more about EpicTide, Inc., visit the company website at www.epictide.com