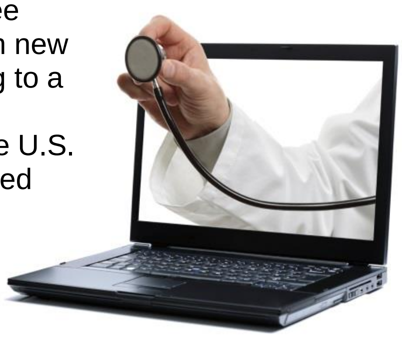
SOMPO INTERNATIONAL

Medical Identity Theft: Fighting an Epidemic

By Brad Gow, Global Cyber Product Leader, Sompo International



Medical identity theft has become more prevalent over the past three years and healthcare institutions now find themselves wrestling with new threats that, in most cases, they had little role in creating. According to a recent study by the Identity Theft Resource Center[1], healthcare organizations comprised 43% of all reported privacy breaches in the U.S. last year, affecting over 4.6 million individuals. Recent medical related privacy regulation, new technologies, the digitalization of personal health records and the introduction of state and federal healthcare marketplaces all ensure that these numbers will continue to grow until comprehensive solutions are found to better protect the integrity of medical data.

The Stakes

Unlike credit card numbers which are easily replaced by financial institutions following a data breach impacting, for example, a retail chain, Personal Health Information (PHI) is tied to an individual's social security number so stolen data retains value for identity thieves long after a privacy breach. Once in a perpetrator's hands, this information is typically used to run medical billing scams or to purchase controlled substances for resale. Stolen PHI can also be used by individuals without healthcare coverage to obtain medical treatment under the victim's name. Over time, victim's health records corrupted with another's medical data introduce new healthcare liability exposures to providers as critical drug allergy or similar data may be missing, incomplete or incorrect.

A More Challenging Environment

Combatting medical identity theft became significantly more challenging over the last year with the rollout of the Affordable Care Act web portal and the various state exchange websites. According to many reports, significant vulnerabilities in the HealthCare.gov website increase the potential for hackers to view and possibly manipulate user data through malicious code attacks.

In addition, the use of cloud storage technology by both network administrators and individual providers has increased by an order of magnitude over the past five years, accentuating the inherent privacy risks associated with this technology. While large vendors typically provide robust, secure virtual storage, individuals storing PHI on easily used consumer applications like DropBox introduce headaches for network administrators tasked with knowing exactly where their organization's PHI is maintained.

Of even greater concern is the implementation – either formally or informally – of 'Bring Your Own Device' (BYOD) policies which allow healthcare workers with access to electronic health records and other protected data to use their own smartphones and tablets in the work environment. A formal information security strategy for these commonly lost or stolen devices is essential and must include technology which allows a network administrator to remotely wipe sensitive information from a device that has been reported lost.

What Healthcare Providers Can Do

Protection against medical identity theft must be closely integrated with a healthcare organization's broader information security and privacy efforts and should incorporate both proactive data protection elements and a comprehensive incident response plan in the event personal health information is compromised. Key components of a privacy program should include:

[1] http://www.idtheftcenter.org/images/breach/2013/ITRC_Breach_Stats_Report_2013.pdf

- Background checks performed for any employee who may eventually be granted access to PHI. Prior criminal convictions for fraud and/or a troubled credit history can identify individuals who might be tempted to steal and resell social security numbers and medical profiles.

- Employee training in the importance of securing PHI and reporting incidences of suspected breaches. Without awareness there is no appreciation for the need to protect sensitive information.

- The latest encryption technology to secure all IT resources, including laptop computers and mobile devices. Where BYOD is allowed, remote data wiping capability must be maintained as well.

- Policies and procedures around the protection of PHI which cover access to information on a strictly 'need to know' basis, robust password management, and guidance on the use of cloud technology.

- Formal protocols to manage all vendors with access to the organization's network which include security reviews, HIPAA/HITECH compliance requirements where appropriate, and contractual protections including the maintenance of cyber insurance.

- An incident response plan incorporating management responsibility for reported breaches and the identification of legal, forensic and other technical resources who are equipped to respond in a timely and professional manner.

Organizations need to make sure they are proactively addressing these risks by developing appropriate medical identity theft protection programs which address both preventative and response actions. A formal, tested response plan can prevent a breach event from expanding into an organizational crisis.

Resources:
Medical Identity Theft. Recommendations for the Age of Electronic Medical Records. October 2013. California Dept. Justice. Privacy Enforcement and Protection Unit.
https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/medical_id_theft_recommend.pdf

Partners in Integrity. Understanding and Preventing Provider Medical Identity Theft. March 2014. CMS. http://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/Provider-Education-Toolkits/Downloads/understand-prevent-provider-idtheft.pdf

Identity Theft Investigation Protocol Checklist. Health Care Compliance Association:
http://www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2007/301-1.pdf

World Privacy Forum Resource Page: http://www.worldprivacyforum.org/resource-page-medicalidentity-theft-information/

This article is a reprint from the Q3 2014 Issue of Endurance Specialty Holdings Ltd.'s Insight and Perspectives newsletter.