THE
NATIONAL LAW REVIEW

Employers Beware: Medical Identity Theft on the Rise and is the Golden Target for Hackers

Friday, December 5, 2014

As we've discussed previously, **medical identity information is worth more than ten (10) times that of financial information on the black market**. This gives **hackers a financial incentive to obtain such information** that is maintained not only by medical providers and pharmacies but also by employers who provide medical insurance coverage to their employees. Employers may hold, in their human resources or other networking systems, not only the medical records of their employees obtained from managing workers compensation claims and other matters, but also, and more importantly, employers may maintain medical insurance registration forms and health insurance billing information on their employees. This is exactly the type of information that is at risk and which increasingly is breached.

Article By Jackson Lewis P.C.
Lillian Chaves Moon
Workplace Privacy Blog

Insurance Reinsurance & Surety
Consumer Protection
Health Law & Managed Care
Communications, Media & Internet
Labor & Employment
All Federal

Why is medical identity information so valuable on the black market? As Fortune reports, medical identity theft is in demand on the black market. Employer data systems are a goldmine for would-be hackers. Within medical records hackers can find social security numbers, dates of birth, health insurance policy numbers, and other billing information that can be used for financial fraud, but also medical identity theft, where the billing information can be utilized to obtain medical services and prescriptions in the name of the individual whose identity has been compromised.

How can employers protect the medical identity information they hold? The starting point is doing a risk and vulnerability assessment to gain an understanding of the business' data privacy and security risks. There are a number of resources available to assist in designing and carrying out an assessment. If the medical information is subject to HIPAA, such as in the case of information maintained with respect to the company's group health plan for employees, HHS has released a security assessment tool. Of course, much of an employee's medical information maintained by an employer is NOT subject to HIPAA, such as leave of absence records and workers compensation records.

Another source is the National Institute of Standards and Technology (NIST) which recently issued a draft update of its primary guide to assessing security and privacy controls. While the work NIST does, including this guide, is designed for federal information systems and networks, it is an excellent and comprehensive source for businesses to understand steps they too can take to safeguard their systems and data. For many employers, these tools may be too extensive and simply not practical. This is where a qualified data privacy expert counselor can add value in helping you to appropriately assess your administrative, physical and technical risks. Either way, a necessary and appropriate risk assessment will then lead to the development and implementation of a written information security program.

Of course, getting management, C-suite, support is essential. Data privacy and security is an enterprise-wide risk which requires an enterprise-wide solution. This is not something that should be left up to the IT Department to handle solo. Rather, the buy-in for the need for adequate safeguards and training has to come from the top and key stake holders have to be brought into the planning and assessment early in the process in order to obtain adequate support for building of data safety program and culture of data privacy and security. Accordingly, the protection of all personally identifiable information, including medical information, takes buy-in and leadership from senior management, a careful understanding the organization's risks and vulnerabilities, knowing what the

law requires, coordination with key persons inside the organization and certain third parties outside the organization, frequent and regular security awareness and training, and regular re-evaluation of the organization's approach for changed circumstances.

Source URL: https://www.natlawreview.com/article/employers-beware-medical-identity-theft-rise-and-golden-target-hackers