

Medical Information Worth 10x More Than Credit Card Data On Black Market

jacksonlewis.

Article By

[Joseph J. Lazzarotti](#)

[Jackson Lewis P.C.](#)

[Workplace Privacy Blog](#)

- [Consumer Protection](#)
- [Health Law & Managed Care](#)
- [Communications, Media & Internet](#)
- [Administrative & Regulatory](#)

- [All Federal](#)

Monday, September 29, 2014

When many people think about identity theft and data breaches, they tend to think about credit card data and bank accounts. This makes sense given the large-scale breaches in the news lately. However, [Reuters reported last week](#) that medical information is "worth 10 times more than [] credit card number[s] on the black market" a trend that has been developing for some time. This makes health care providers and their business associates increasingly likely to be targets of an attack. Small businesses in this industry are not immune as even a solo practitioner can amass data on thousands of patients. See [NYT article](#) making this point and providing some helpful strategies.

Like financial institutions, insurance companies, and retailers, businesses in the healthcare industry maintain vast amounts of sensitive data including health insurance policy numbers, social security numbers, birth dates and other billing information, not to mention sensitive diagnosis information. As healthcare costs continue to rise, the opportunity to use another's identity, policy or account to obtain healthcare products and services is a strong driver of the value of this data on the black market. In addition, providers and other health care businesses generally are not as advanced as banks and financial institutions in safeguarding individually identifiable health information, or spotting identity theft. As data is not perishable, and this sector is reported to generally be slower in reacting, identity

thieves tend to have a longer time frame to use the information.

The increasing exposure for businesses in the healthcare industry is evident in recent studies by the Ponemon Institute which show cyber attacks have risen from 20 percent in 2009 to 40 percent in 2013, as noted in the Reuters article. Other [reports](#) highlight increases in HIPAA breaches. See also [MelaMedia's](#) helpful collection of statistical information concerning HIPAA data breaches and other metrics.

Clearly, the healthcare industry will need to continue to address this increasing threat, although static budgets and strapped resources of course present significant challenges. For organizations that have not already worked through a HIPAA compliance program, there is a bunch of low hanging fruit that can be adopted with relative ease and low expense to safeguard data. Creating adequate safeguards and a culture of privacy and security does not happen overnight. It requires 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.

Jackson Lewis P.C. © 2019

Source URL: <https://www.natlawreview.com/article/medical-information-worth-10x-more-credit-card-data-black-market>