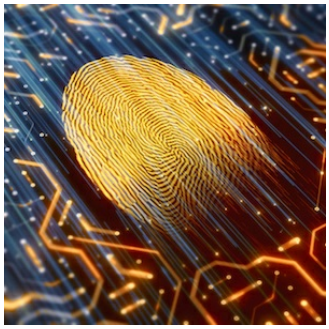
HealthManagement
Promoting Management and Leadership

How to Secure Sensitive Healthcare Data



In today's highly interconnected world, securing and protecting sensitive data can be a big challenge. This is even more true in healthcare, where data protection can become a matter of life and death.

Encryption is considered one of the most effective ways to protect data. As noted by the Ponemon Institute, about half of healthcare and pharmaceutical companies use data encryption in one form or another.

You might also like: **Ten Ways to Keep Your Networks Hacker Proof**

Some healthcare organisations, for example, apply encryption at their internet connections or computer workstations. For others, the focus is on the protection of their databases.

Indeed there is currently no single or standardised approach in data encryption. Notably, the key to effective encryption is effective key management, according to data security experts,

Shachar Roth, VP of R&D at Kindite, highlights the importance of "customer-centric encryption" in healthcare. To make this concept work, he says, "healthcare organisations must consider how easy it is for patients, employees and business associates to use and trust the encryption solution."

For Roth, an effective key management strategy includes these elements:

- **Key Storage**: to ensure that no one can steal your keys.
- **Rotation/Destruction of Keys**: to ensure new keys are applied to new data sets, while preserving the old keys for older sets.
- **Key Generation Granularity**: enabling a zero trust approach while still providing access to the lowest tier of authorised users.
- **Automation**: improving the speed of key management while easing the burden on administrators and reducing mistakes.
- **Ease of Use**: even the most feature-laden key management system is ineffective with a poor user interface.

With the broadening adoption of blockchain technology in healthcare, such as in records management and billing, there is all the more reason for organisations to put a Key Management Programme in place. While a blockchain may create a tamper-proof record of transactions, experts say the system must still be restricted to authorised users.

Key management requires a few tweaks when it comes to blockchain, including the need to work with non-standard cryptography and the ability to incorporate multiple keys into multiplatform environments, according to Jason Sfaelos of Equinix, a company that specialises in internet connection and data centres.

Source: Techopedia
Image credit: iStock

Published on : Thu, 27 Feb 2020