Data Security: Keeping Your Data Secret and Sacred

Ivana Popovic January 09, 2019

With the digitalization of the healthcare industry comes the need for greater security.

You were warned that one day everything would be digital, and that day has arrived â€" paper is now useless in many applications where it was once a necessity.

(Newswire.net -- January 9, 2019) -- You were warned that one day everything would be digital, and that day has arrived — paper is now useless in many applications where it was once a necessity. The digitalization of data has completely changed the way records are kept and shared in the healthcare field. Today, these operations run more fluidly than ever, allowing healthcare providers and administrators to better log patients and their treatment.

But technology growth introduced some risks as well. Never before has data been so vulnerable to security breaches, and there are literally people who make their living by stealing and selling data. With the digitalization of the healthcare industry comes the need for greater security. Here are some tools and practices to help you secure your medical data.

Set up permissions on your network

If you are a healthcare administrator, or you own your own practice, data security must be one of your top priorities. It needs to be established early on who has access to what data. Limiting access to certain data to certain individuals is a form of addition by subtraction. When your data is compartmentalized, it adds a layer of accountability. If you find that a security breach or data discrepancy is not of outside origin, then its source is one of the people in the department that has access to it.

Additionally, limiting access to data on a need-to-have-it basis is a good safeguard against human error. This falls in line with the old saying about how “too many cooks in the kitchen spoil the broth”. In the hands of too many users, even competent ones, data is susceptible to error or corruption. Keeping traffic to a minimum ensures that data is accessed and altered less, meaning that there are less opportunities for mistakes.

Get outside help

Because of the prevalence of digital network technology, many companies decided to hire IT teams to manage their network. This is a practical solution, but it’s also a very expensive and time-consuming one. Businesses spend a large amount of their time and money hiring and training new recruits. However, hiring and training IT specialists is a pain that you can avoid by outsourcing your IT department, which saves time and money.

Another benefit of outsourcing your IT department is that you have access to the latest industry software. You won’t have to worry about updating hardware and software, because the contracted company does that for you. Plus, the company that you turn to has already done the hard work of finding and training the right people for the job. Experienced data management companies like Liaison Technologies provide you with top-notch solutions to not only secure your data, but help improve operations and care efficiencies as well.

Lock it down like Fort Knox

The internet is not the only means by which a hacker could steal your data. It is crucial that you have trained IT specialists and great software to defend your data, but you would be remiss if you did not consider physical threats to yours and your patients’ data. Make sure that you apply strong locks to file cabinets and office doors. Strategically place cameras to watch areas where data is stored. Most importantly, your server should be in a secure room with limited access to it.

As a healthcare provider, your responsibilities are numerous. However, aside from the well-being of your patients, your greatest responsibility is the security of their information.

Source: http://newswire.net/newsroom/blog-post/00106853-data-security-keeping-your-data-secret-and-sacred.html