

What You Don't Know CAN Hurt You!
By Brad G. Storey, MSW
Director, Risk Management Division | Irwin Siegel Agency, Inc.

How many USB flash drives or other forms of removable storage are floating around your organization? If you know the answer to that question, try this one: what is on those USB flash drives or other removable storage? Don't feel like you are alone if you're not sure. This is perhaps one of the most rapidly growing exposures for human service providers. With increasing legislation around identity theft and tighter privacy laws, removable storage devices pose a major threat and need to be accounted for in your risk management planning.

In 2010, The Ponemon Institute released a study on the cost of data breaches, revealing the average cost per compromised record to be about \$214. In November 2011, a physician's network in northern California reported a laptop stolen that contained more than 4 million patient records including names, addresses, phone numbers, and insurance information. The laptop and other computers on their network were not encrypted. Based on the data provided in the Ponemon report, this incident could cost as much as \$856 million! While most non profit organizations do not serve 4 million individuals, this example serves to identify how quickly costs can add up when it relates to data breaches. In addition, it is extremely difficult to quantify the impact of indirect costs, such as damage to an organization's reputation and goodwill within their community.

In many organizations, flash drives and other means of removable storage (netbooks, smart phones, tablets, etc.) can bypass established security measures such as firewalls and antivirus applications. Whether intentionally malicious or not, users may unleash viruses onto the network which may cripple it for days or cause security holes. Though these devices are small, portable and convenient, they are also easy to misplace and if not protected correctly, the information on the drive may be exposed. As demands of accurate and timely documentation increase exponentially, community providers are at an increased risk. In an effort to comply with regulatory bodies, many case managers and human service employees document services at home or a satellite location and store their notes on a flash drive. If a typical community case manager serves 15 individuals, and you have 10 case managers all using flash drives, 150 individual's confidential information could be at risk.

Prior to use of any removal storage device, the organization should have it scanned for viruses. Organizations should establish an acceptable use policy covering the use of flash drives within their networks. The policy should mandate that all users who require the use of a flash drive obtain some form of authorization prior to using the device. In an effort to minimize the loss of sensitive information, the organization should establish a minimum level of encryption to protect the data. In addition, the policy should also require a file on the drive with contact information which can be used to return the device to the organization as well as a legal disclaimer that the information on the drive is private and confidential and is protected by law.

It is important the information your usage policy be covered during the on-boarding process to any organization. This should include the potential risks and liability of the individual who may inadvertently disclose the information.

Like other exposures in human service provider organizations, even the best controls may not completely eliminate the potential for a loss. Organizations should consider a robust cyber liability policy that extends to electronic information on flash drives and other removable storage devices.

For more information, visit: <http://www.siegelagency.com/insurance-programs/netprotect-cyberliability/> or contact one of our product specialists.

Rich Geoghan: rich.geoghan@siegelagency.com or 800.622.8272 x5142

Elizabeth Friedman: elizabeth.friedman@siegelagency.com or 800.622.8272 x5135