Best Practices

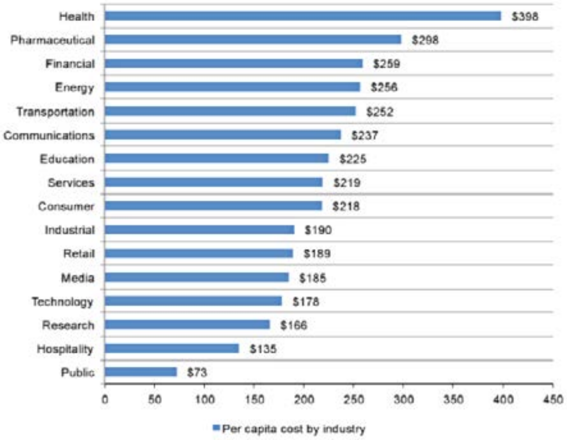
Healthcare & Encrypted USB drives

Healthcare companies of all sizes are challenged by the task of securing the data generated and collected about the patients they serve. This data comes in many forms, but we will focus on the data transported outside the network. Any data that is produced, saved, transferred or received in electronic form is considered to be electronic protected health information, or ePHI.

USB Flash drives are an easy and efficient way for providers to transport patient data from one office to another, or to an offsite hospital or care facility. They make it easy to bring data along for further analysis or for consultations.

Unfortunately, even though they are inexpensive and easy to use, USB drives can also put your organization at risk of non-compliance for HIPPA. Any data stored either short- or long-term on a USB drive is considered to be electronic protected health data and subject to the same storage, transportation and data destruction rules as other storage media used by a health care organization. The loss or theft of the drive is considered an automatic breach and is required to be reported and affected patients notified — and could even require public notification.

According to the Ponemon Institute, the average cost per organization for a data breach was up to $217 per lost or stolen record. The average cost for a healthcare organization jumps to $398 per record. Those costs factor in both the direct costs associated with a breach such as fines, legal expenses and victim identity programs, as well as the indirect costs such as customer/patient churn and public perception. Suddenly that USB drive has become very expensive



DataTraveler Vault Privacy 3.0 Anti-Virus
DataTraveler Vault Privacy 3.0
DataTraveler 4000 G2

Kingston's encrypted drives use industry-leading 256-bit AES hardware encryption and require complex passwords to access the data stored on them. If they are lost or stolen, the data cannot be accessed. If the attempted breach was a malicious attack, which about half are, the organization can rest assured knowing that the Kingston drive locks down after 10 invalid login attempts. Using encrypted USB drives is considered to be a reasonable step to prevent a data breach incident and can be a positive communication in the event of an incident.

more ››

Not all USB use is innocent. USB drives can be used by attackers to take data from an organization. A good policy to put in place is "whitelisting" devices on USB ports within your network. This allows approved devices to be used while blocking those not on your lists from gaining access to those data ports.

Kingston's encrypted USB drives can be added to an organization's current endpoint solution by using the unique Product ID number to allow these drives to be used within the network. Kingston also offers some additional features to IT teams like Dual Password and Anti-Virus protection. Dual Password allows an IT administrator to configure the Kingston USB drive with an administrator password before handing it off to staff. By doing this, the IT team can access drives if a director forgets his or her password.

Kingston also has an Anti-Virus model that scans the electronic data on the drive for viruses or malicious files. If a data breach is malicious, the attacker may use a virus, a common tool for hackers. Kingston's encrypted drives cost between $25 and $250, depending on capacity. For health care organization facing costs in the millions if a data breach occurs, the Kingston drives are a small investment to help all healthcare organizations secure those millions of dollars as profit instead of losses.