LOK-IT
SECURE FLASH DRIVE™

BACKGROUND

KAISER PERMANENTE: A MANAGED HEALTH CARE ORGANIZATION

Kaiser Permanente is the largest managed care organization in the United States.

Kaiser has 8.7 million health plan members, 167,300 employees, 14,600 physicians, 35 medical centers, and 431 medical offices. In its most recently reported year, the non-profit Kaiser Foundation Health Plan and Kaiser Foundation Hospitals entities reported a combined $42.1billion in operating revenues.

HIPAA COMPLIANT

If you would like to see how simple it can be for your healthcare facility to secure portable data, we'd be happy to send you an evaluation LOK-IT at no charge.

Executive Case Study:

LOK-IT and Kaiser Permanente

KAISER PERMANENTE®

***Issue for Kaiser*: USB flash drives necessary for data storage**

Use of USB flash drives for transporting and storing sensitive information are often critical to many Kaiser processes and help to increase productivity. However use of typical USB flash drives created challenges in two key areas which Kaiser needed to address.

The first challenge was protecting drive content. HIPAA and HITECH regulations state that if patient records are lost and are not encrypted properly, then the organization can be subject to $1.5 million in federal penalties, among other very large costs associated with the breach.

***Solution*: LOK-IT Secure Flash Drive®**

In order to decrease both the liability and the possibility of data breach of patient data, Kaiser implemented an enterprise data protection and encryption solution. This solution has a feature which utilizes proprietary software to encrypt data saved to removable media. However, like all such network-based data protection solutions, its use caused USB flash drives to lose their flexibility as the software used to encrypt drive content made them platform dependent and inoperable on Kaiser's PCs.

The second challenge was addressing the fact that USB connectivity has become the standard for many types of devices such as scanners, projectors and medical equipment, not just computers that are usually equipped with a keyboard or touch screen and a standard Windows or Mac O/S. The software encrypted USB drives were inoperable on much of this new USB compatible equipment. Personnel in a variety of positions at Kaiser needed to access data from an encrypted flash drive but were unable to do so with their current enterprise solution.

After thoroughly evaluating the LOK-IT Secure Flash Drive®, IT management found LOK-IT was the right solution to enable Kaiser employees to utilize portable data securely when their enterprise solution fell short. LOK-IT's use of hardware authentication via onboard PIN Pad* and 256-bit AES hardware encryption eliminated the flexibility issues previously experienced. Kaiser had implemented strict port management controls so as to only allow permitted devices to operate on USB ports connected to the network, and now added LOK-IT to the white-list of removable devices. Today, Kaiser employees across the country are using LOK-IT for a wide variety of purposes:

*Kaiser Health Education trainers use projectors that have USB ports. Since there is no way to type in a password (projectors have no keyboard) and no standard operating system, only a device that uses hardware authentication can be utilized. Traveling training personnel can have their presentations stored on LOK-IT and then simply plug LOK-IT into the projector when needed.

*Physicians needed to access medical records that were stored on pacemakers and implantable cardioverter defibrillators, such as the devices manufactured by St. Jude Medical. These devices are equipped with USB ports for offloading data, and now LOK-IT can be used to perform this function securely.

*Kaiser Foundation Hospitals Center for Health Research found LOK-IT to be the only flash drive that they could use to securely transfer files between their Linux and Windows computers.

*Kaiser IT personnel use LOK-IT to transfer files between Windows computers and other equipment. This equipment includes Kodak scanners and BioMedical equipment.

*Based upon DataLock®, licensed technology from ClevX, LLC – Patents Pending