

SECURE USB DRIVES IN THE NHS

Hospitals face a daily challenge to be more efficient, but without putting patient and other sensitive data at risk.

With staff at NHS trusts often working across multiple sites, and often an urgent need to transfer patient data from one place to another, using USB drives and other portable devices is hard to avoid. At the same time, trusts do not have unlimited budgets to introduce complex security measures.

West Suffolk Hospital NHS Trust is one of the early adopters of encrypted USB memory devices. The trust, which runs the West Suffolk hospital in Bury St Edmunds, introduced around 150 SafeStick USB drives, from vendor BlockMaster, last November. BlockMaster has since won a two-year contract with the NHS to supply up to 100 000 of the devices.

"USB sticks are the most convenient method of transporting information", says Mel Hodson, IT procurement manager for West Suffolk Hospital NHS Trust. "Generally we have used the sticks, but with confidential information going via NHS email. Now, we are a lot happier if a SafeStick is mislaid. We can lock down a SafeStick using the software, so that nobody can use it. Once that's happened, it can't be accessed by anyone." Staff are also unable to copy sensitive data to standard USB drives.

End users can reset the PIN on a SafeStick if they forget their details, but doing so erases its content; however, the IT department can reset the device and preserve the data. "We have reset a few, but we've not had to block many sticks", Hodson says.

Indeed, now that the trust uses secure memory sticks, it has seen fewer losses. "It has been the reverse, in fact", says Hodson. "You have to sign to take a stick out, and users are being a lot more careful. The cost is higher with an encrypted stick, but it is also making departments think twice about how many people will be issued with them."