

Customer Success Story



NHS Scotland

Combining Best Practice with Best Value Across NHS
Scotland - NHS National Services Scotland Joins
Forces to Procure Lumension Security Software

Introduction

Following several high profile cases of the loss of person identifiable data by English Government departments, the Cabinet Office published the “Data Handling Procedures in UK Government” report in June 2008. This highlighted the need to restrict access to public sector data and encrypt data held on removable storage media such as CDs, USB keys and laptops. The report led to rigorous product specifications being developed for the procurement of information security products by public sector departments throughout the UK. In response to the report, the Scottish Government made £1million available to the Scottish Health Boards to enable them to comply with the latest data handling requirements.

Protecting Data Across NHS Scotland

Mark Salveta heads up the team in NHS National Services Scotland who provide IT software procurement support to Health Boards and is responsible for ensuring that the best value for public money is delivered when new information security products are being sourced for the 22 health boards that serve Scotland.

“The new policy demanded that all 22 Health Boards acquire products enabling them to encrypt personal data stored on mobile devices such as USB storage keys and laptops. The definition of ‘personal data’ has a wide scope and includes any information such as clinical records or names and addresses of individuals or businesses, as well as the more obvious issue of patient confidentiality.”

Mark Salveta, NHS National Services Scotland

As part of its remit to gain the best return on the Scottish Government’s investment, NHS National Services Scotland facilitates the combined purchasing power of all 22 health boards. Mark Salveta explains that there are 158,000 NHS staff working within the 22 Scottish Health Boards and 92,000 desktops that need to be protected. For examples: Lothian has 12,000 desktops and 20,000 staff; Grampian has 8,000 desktops and 10,000 staff; NHS Lanarkshire has 7,000 desktops and 9,000 staff; NHS Orkney and NHS Shetland each have 500 desktops to protect.

Explaining the product sourcing arrangements across NHS Scotland, Salveta says: “NHS National Services Scotland already had an agreement with TrustMarque Solutions, which had won the NHS tender two years earlier. So we already had data protection products in place through this supplier.”

NHS Scotland’s main requirement was to source a product that could help to control the storage of personal data on removable storage media such as USB keys, laptops and CDs. “We need to be able to know what data is being accessed, moved and stored and by whom. The protocol should be that nobody takes data outside of the hospital or GP’s surgery.” states Salveta.

“Essentially, we needed a product that would prevent anyone from storing patient data or any other health board information, onto a CD, DVD, USB stick or laptop, without having express permission to do so.”

Mark Salveta, NHS National Services Scotland

The Information Commissioner’s report also specified the need to encrypt data where it was necessary to store it on removable storage media.

“There have been instances of laptops being stolen from government employee’s cars in England and Scotland. We needed a product that could prevent large chunks of information from being popped into someone’s pocket and taken out of the door. Where this method of data transfer was sanctioned, we needed to know that the information was encrypted.”



Following the Information Commissioner’s report, NHS National Services Scotland looked at the English specification and approved this with Scottish NHS IT specialists. IT then undertook a rigorous product evaluation process in which Mark Salveta and his team specified recommended products for the NHS Scotland based on their features, cost and service. “Essentially, this was an exercise to ensure that all 22 Health Boards were able to access the best security products at the best price. We reviewed products from 10 vendors using a technical score; cost; and the quality of vendor’s service and Lumension scored the highest,” says Salveta.

Salveta says. “The Scottish Health Boards still have the option to choose a different product, but all 22 Boards have an obligation to comply regarding the protection of data stored on portable devices.”

Lumension’s device control software enforces NHS security policies through its “default deny” approach, creating an IT environment in which no data can be transferred from the server to a laptop, CD, DVD or USB storage device, without the

express permission of the IT manager. This allows the IT manager to pinpoint exactly which employee has transferred files and reinforces the responsibility of named NHS employees to protect the data that they are transferring. In addition, Lumension's integration with PGP ensures that authorised data transfers can be encrypted on laptops and other portable storage media.

Lumension provides centralised control, giving NHS IT teams total visibility of all data transferred to removable storage media. It allows IT managers to specify exactly which devices can be connected to the network, blocking all others by default. This feature is sufficiently granular to restrict data transfer to specific USB keys with specific serial numbers. An auditing feature within the product can create a report of all devices that have ever been connected to a department's network and flags up any attempted connections. The software also enables NHS Health Boards to quickly create reports to demonstrate compliance with Government legislation regarding secure data handling.

IT managers can also use Lumension to set file copy limits, to prevent entire databases being moved onto portable devices, even by authorised employees. Certain file types can be blocked from being transferred. So for example, an authorised NHS employee could store Word documents onto an encrypted USB stick, but be blocked from copying image files onto the same stick. Using Lumension, IT departments have absolute control over the storage of data onto portable devices.

Ted Boyle, Systems Administration and Security Manager for NHS Lothian describes the Lumension implementation process as one of education first and deployment second:

"We first installed the software in September last year, but before rolling it out, we had to find out exactly what devices were being connected to the network. We started by using Lumension to 'listen' to the network to find out exactly which devices were being used by NHS staff. Once we had that visibility, we specified which devices could be used and spent the next three months educating staff about how to use devices securely and explaining the changes that would be brought about once Lumension was rolled out. I must make clear that even before Lumension was installed, the NHS Lothian policy was to forbid anyone from storing patient data on removable storage devices."

Ted Boyle, Systems Administration and Security Manager, NHS National Services Scotland

Ted Boyle believes that this user education process was crucial for ensuring a successful deployment. His team raised awareness of the security issues posed by removable storage devices and communicated how Lumension would change NHS Lothian's use of these devices, using a variety of media including articles in the NHS Lothian newspaper; workshops; and team briefings within NHS

Lothian. He also organised road shows where junior doctors and other NHS Lothian staff could collect an authorised, encrypted USB storage pen.

“We purchased 4,000 USB pens and encrypted them using Lumension. This represents a ratio of one USB device to 7.5 members of staff. We are a major teaching and training organisation, so these devices are used for this purpose rather than for storage of patient data. Through our staff education programme, the initial misapprehension felt by staff at losing their ‘right’ to use portable storage devices, gave way to acceptance that using only authorised, encrypted pens would still allow them to get on with their jobs, without posing a risk to data”, reports Boyle.

“Lumension’s Device Control software adds an extra layer of protection, to enforce the existing policy preventing staff from storing patient data on portable devices. Where it is absolutely necessary to store patient data, NHS Lothian staff still need to get approval to do so and this permission is facilitated via Lumension Device Control. So we always know which member of staff has patient data on his or her USB pen.”

Ted Boyle reports that following NHS Lothian’s user education programme, Lumension was rolled out to 9,000 desktops in January 2009 and has been running smoothly ever since:

“The key benefit is that it has made our data safer.”

Ted Boyle, Systems Administration and Security Manager, NHS National Services Scotland

Continued »

Key Benefits:

Salveta reports that using Lumension's Device Control software, the Health Boards in Scotland are able to protect all removable storage devices as well as enabling Scottish NHS providers to encrypt any data that has to be stored in this way. "At present the software is mainly used to prevent data being moved to USB storage keys and laptops. We are also looking at whole disk encryption. The product has been used for a couple of years by individual health boards at departmental level to encrypt data stored on laptops. We have had very positive feedback from the Health Boards such as NHS Grampian, that have deployed Lumension, both in terms of product capabilities and the level of service provided by the vendor."

Lumension has been able to support and enforce the device control and data encryption policies for a number of health boards that are using different IT systems. Health Boards have to be able to communicate with a variety of legal entities, including a board of representatives chosen from local communities and businesses, so it was important that any product installed by the NHS Services Scotland could support a variety of operating systems and hardware.

"The Scottish Health Boards for each area have an element of local power, so it's good to see them come together to negotiate the best price through NHS National Services Scotland," comments Salveta. "By combining their purchasing power, the boards have managed to get at least twice the amount of product that they could have bought individually."

Mark Salveta explains that one of the major benefits of installing Lumension Device Control with PGP encryption is the peace of mind it provides to IT managers across NHS Scotland and reassurance for members of the public that their data is being looked after:

"With Lumension installed, we know that if any device goes missing, the data on it will be encrypted and we will know exactly who stored what onto it."

Mark Salveta, NHS National Services Scotland



Global Headquarters

15580 N. Greenway-Hayden Loop, Suite 100

Scottsdale, AZ 85260 USA

phone: +1.888.725.7828

fax: +1.480.970.6323

www.lumension.com

Vulnerability Management | Endpoint Protection | Data Protection | Reporting and Compliance