

# Customer Success Story

**Barts and The London**   
NHS Trust

Barts and The London NHS Trust Partners with Lumension  
to Strike Gold with its Compliance and Data Protection  
Strategy

Barts and the London NHS Trust Adopts Award-Winning  
Lumension Data Protection to Set a Strong Security  
Foundation and Prepare for the 2012 Olympics

## Overview

Barts and the London NHS Trust comprises three hospitals: The Royal London in Whitechapel, The London Chest hospital in Bethnal Green, and Barts and the London NHS Trust, situated by St. Paul's in the City.

These hospitals have been at the centre of the development of medical and surgical history since the 1500s, with many famous surgeons, bacteriologists, anaesthetists and nursing staff emerging from their wards. Today, Barts and the London NHS Trust is a major teaching hospital and a centre of excellence for oncology, surgery, cardiac care, fertility treatment and paediatric care. It has been ranked among the top hospitals in the UK for clinical quality and safety.

The Trust is also home to the London air ambulance and is the capital's leading provider of emergency and trauma care. Barts and the London NHS Trust is undergoing the largest and most complex hospital redevelopment project in the country.

The Royal London will be Britain's largest new hospital, providing general and specialist services to the population of east London and beyond. The historic buildings of Barts, Britain's oldest hospital, will be refurbished, alongside a major new building, to create a Cancer and Cardiac Centre of Excellence.

The new hospital's project is integral to wider plans for modernising health services across east London, supported by state-of-the-art technology and facilities.



Alan Freedman is a senior security engineer at Barts and the London NHS Trust, where he is responsible for IT security. Part of Freedman's role is to identify and implement solutions to assist in maintaining the Trust's ISO 27001 registration.

ISO 27001 is the audited management function of ensuring that information security systems are adopted throughout an organisation. The standard requires that an organisation has taken account of all vulnerabilities, threats and the impact of breaches and has taken specific steps to address these and reduce risk to the organisation. The standard requires a comprehensive management process designed to minimise risk to hardware, software, networks and paperwork on an ongoing basis and to protect against existing and emerging threats. Barts and the London NHS Trust has a full audit every three years undertaken by BSi and a continual audit every six months to ensure that the IT systems management is in line with ISO 27001.

## The Challenge

Freedman explains that computer virus infection is still a major risk that has to be managed by Barts and the London NHS Trust on an ongoing basis. Following a virus infection on the Trust's network in 2008, the Trust supplemented its McAfee antivirus software by introducing Tipping Point as well as Blue Coat AV at the gateway to protect against viruses carried via incoming Web and e-mail traffic. This traffic is run within a sandbox first to enable Freedman and his team to identify whether anything poses a threat before allowing it onto the Trust's network.

Another source of virus infection is from portable media such as USB memory sticks being plugged into laptops and PCs on the corporate network, as well as potentially virus-laden CDs and DVDs being brought in from outside and introduced on the Trust's hardware. These needed to be managed as part of the Trust's overarching information security policies.

Another challenge cited by Freedman is the need to prevent sensitive patient information from being stored on removable storage devices. Initially, Barts and the London NHS Trust installed McAfee Safeboot to lock down the Trust's laptops. This was in response to a number of high-profile incidents in other public and private sector organisations.

"We had already protected the laptops, but this wasn't enough. We needed to be able to control external removable devices, such as USB sticks, cameras and MP3 players, as well as encrypting the data stored on laptops," Freedman says.

"iPods and iPhones, for example, are blocked because it is hard to detect whether it is electricity or data that they are downloading when they are plugged into a Trust PC. This could be as much as 160GB of removable storage, so there is a security risk posed by these devices. I have also had conversations with photographers about the large storage capacity of digital cameras, and the potential risk that they pose to patient data. Of course, photography is required, for example, for images taken before and after surgery, so that consultants can review the progress of a patient's treatment. What we needed was a way to stop these massive portable storage devices from being used for unauthorised or malicious purposes."

**Alan Freedman, Sr. Security Engineer**  
**Barts and the London NHS Trust**

## The Approach

Under Freedman's recommendation, the Trust investigated alternative products that would enable the Trust to develop and enforce information security policies while enabling specific staff to store data onto AES256 encrypted Integral or SafeStick USB memory sticks, to facilitate medical care and teaching roles. The Trust identified Device Lock and Lumension Device Control as the two leading endpoint security products on the market. After a

rigorous selection process in line with ISO 27001, Freedman recommended that Barts and the London NHS Trust install *Lumension*® Device Control, industry's leading whitelisting technology.

Lumension Device Control prevents data loss or theft by enforcing an organisation's policies regarding the use of removable storage devices, including CDs/DVDs, USB memory sticks, digital cameras and MP3 players. The software enables the IT team to centrally view and control every device that can connect to the Trust's PCs, workstations or laptops. *Lumension*® Data Protection Solution allows the IT staff to discover every device that has ever been connected to the network. This is important for identifying and addressing any known vulnerabilities.

A key feature of Lumension Device Control is that it applies a "whitelisting" technology, enabling an organisation to clearly specify which removable storage devices are allowed to be used — right down to the product serial number. All other devices are prevented from being connected to the network. Where additional devices are permitted, such as to enable an individual employee to carry out a specific task, all data transferred to or from the device may be audited by the software, and a copy of the data can be created using Lumension's patented bi-directional Shadowing Technology.

Freedman explains that local initiatives on secure data handling have forced the use of encrypted USB sticks from specified suppliers. This has made

the creation of the whitelist a lot more straightforward and expedited the implementation of Lumension Device Control across the Trust.

Freedman reports that in spite of government moves to ensure that all of the public sector staff is following common guidelines on encryption and data handling procedures, there are still instances of people using non-sanctioned USB storage devices.

"We used the software to check what had been connected to the network historically, and there are a huge number of devices that have been plugged in. Lumension Data Protection Solution allows us to enforce policies by blocking everything except the SafeStick or Integral devices. Using Lumension, we can centrally control how data is moved and stored around the Trust's system and check whatever has been copied to devices."

**Alan Freedman, Sr. Security Engineer**  
**Barts and the London NHS Trust**

Once the whitelisting technology has been employed to enforce policies on the use of removable storage devices, Lumension Device Control allows the IT team to monitor the permitted and attempted use of devices on an ongoing basis. This allows them to identify potential threats. For example, where repeated attempts have been made to connect a prohibited device, this may alert the IT team to a risk of data theft.

For reporting and compliance purposes, Lumension Data Protection creates an audit trail of all data that has been moved to or from removable storage media. IT managers can also use Lumension Data Protection to set limits on the type and size of file that may be transferred to sanctioned devices. This prevents large chunks of data from being removed from the organisation without making sure that data handling procedures, such as full disk encryption, are being followed to the letter.

“We selected Lumension Device Control because it provided us with a granularity that offers complete control over the majority of the Trust’s IT devices, while allowing exceptions to that rule where required. For example, we can say that for a single person or a group of people they can use a specific device to undertake tasks as required by their role,” Freedman explains. “With this granularity and the integration with Active Directory, Lumension Device Control stood out from the competition.”

## The Solution

Barts and the London NHS Trust went live with Lumension Device Control in October 2009. The countdown to the USB device policy enforcement was communicated to staff via the Trust bulletin and an all-staff e-mail.

Freedman reports that SMS was used to deploy Lumension Device Control across the Trust’s IT estate and that this made it extremely straightforward. “SMS has been used to deploy Lumension

Device Control reasonably quickly. It has taken just over a month to install the software on 4,500 PCs across the Trust,” Freedman says.

“We really value the fact that Lumension Device Control integrates so well with Active Directory. This made the implementation a lot easier, particularly where we’re trying to create different rule sets for different user groups. Effectively, everyone is blocked from using removable storage devices, but you can allow privileges where necessary. Centralised control is very useful if you want to know what people are doing with the Trust’s data. It is also vital for our reporting and auditing as part of our ISO 27001 compliance,” Freedman says.

## Key Benefits of the Implementation

Freedman cites the key benefit of gaining full visibility of the transfer of data throughout the network, with centralised control and full reporting functionality. The financial benefit of being able to control exactly which devices are plugged into the Trust’s network is the avoidance of a potential £½ million fine imposed on organisations if they are found to be negligent. But beyond that, Freedman says: “The installation of Lumension Device Control to protect all 4,500 endpoints has provided us with peace of mind. It’s hard to quantify the return on investment gained from being able to provide effective insurance against data loss or data theft perpetrated through using removable storage devices. How do you quantify the benefits of protecting the public’s data and the Trust’s reputation?”



**Global Headquarters**

8660 East Hartford Drive, Suite 300

Scottsdale, AZ 85255 USA

phone: +1.888.725.7828

fax: +1.480.970.6323

**[www.lumension.com](http://www.lumension.com)**

Vulnerability Management | Endpoint Protection | Data Protection | Compliance and IT Risk Management