Confidence in a connected world. ✓ Symantec™

Bedford Hospital NHS Trust

Best-in-Class Data Loss Prevention for U.K. Healthcare Trust

The Information Commissioner's Office (ICO) recent powers to serve monetary penalties of up to £500,000 ($785,000) for serious breaches of the Data Protection Act and the recent fines to public sector organisations has been a wake-up call for the U.K. healthcare sector. It has never been more important to discover, monitor, and protect confidential electronic healthcare data. Bedford Hospital NHS Trust in the U.K. is at the vanguard of this electronic data loss prevention revolution, introducing Symantec™ Data Loss Prevention to introduce universal policies for data loss prevention, monitor the movement of confidential data across the NHS Trust, and ensure an even greater degree of confidence in the data. The unified solution is being used to highlight the potential improvements which could be made to business processes for transmitting confidential data—such as patient records, employee information and Trust data—and ensure the hospital is not exposed to fiscal penalties for data loss from the ICO.

ORGANIZATION PROFILE

Website: bedfordhospital.nhs.uk
Industry: Healthcare
Headquarters: Bedford, U.K.

SYMANTEC SOLUTIONS
Data Loss Prevention
Web Security
Information Risk & Compliance

Protecting healthcare information from loss

"The health service holds highly sensitive patient information, therefore it is vital that organizations across this sector make sure their data protection practices are adequate." Not the words of Symantec, but the words of Dawn Monaghan, Strategic Liaison Group Manager for Public Services, at the ICO in the U.K.

The importance of safeguarding medical data is not lost on Mark Austin. As the chief information officer (CIO) for Bedford Hospital NHS Trust, a high-performing acute district general hospital Hospital he and his team are responsible—among many pressing tasks—for ensuring that confidential patient data is protected from loss.

"Protecting patient data, employee information and Trust data is a challenge which is faced by all NHS Trusts including Bedford Hospital. Bedford Hospital has policies in place to determine what data can and can't be stored or transmitted by email and this system will ensure that these policies are adhered to."

Why Symantec?

· Quality of Data Loss Prevention Risk Assessment

· Straightforward platform customization

· Experience of Symantec in information risk and compliance field

Eliminating exposure to monetary penalties

There's good reason for doing this. Besides the moral obligation to respect the confidential nature of patient data, NHS Trusts could be served a monetary penalty by the ICO should a serious breach of the Data Protection Act occur.

Bedford Hospital is ahead of the curve here. The NHS Trust has taken the strategic decision to deploy Symantec Data Loss Prevention to discover, monitor, and protect confidential Exchange email traffic wherever it is stored or used. This best-in-class risk management solution replaces an assortment of mail MTA filtering and proxy web filtering tools and is used to scan Internet email and other outbound Web traffic to prevent loss of confidential data.

Striking the right balance between freedom and confidentiality

"One of the main reasons for choosing Data Loss Prevention is the ability to configure the solution," says Austin. "It strikes just the right balance between giving staff the freedom to work and locking down confidential information. For example, staff can send out a patient hospital number, but that email could not include any other personal identification details or healthcare information. Like everyone else, we also filter out most websites of a sexual nature, but permit ones that support medical learning and patient care."

Another key advantage of Data Loss Prevention is the seamless integration into the NHS Trust's current environment. Austin's team now has the scope to check every email and where it is going. They can also define universal policies across the Trust, remediate and report on incidents, and detect content accurately within one unified platform.

The starting point for the implementation has been a Symantec Data Loss Prevention Risk Assessment, which allowed Bedford Hospital to quantify and qualify their risk of data loss. It answered questions such as, 'How much and what type of confidential information is exiting the network? Who is transmitting confidential information outside the Trust? And what network protocols carry the most violations?' "The Data Loss Prevention Risk Assessment monitored our email traffic and highlighted potential areas of data loss. This provided us with the necessary information to create a business case," says Austin.

SOLUTIONS AT A GLANCE

Key Challenges
- Make sure data protection practices are adequate
- Avoid fiscal penalties for non-compliance
- Meet moral obligation to respect patient confidentiality

Symantec Product
- Symantec Data Loss Prevention 11.5

Technology Environment
- End users: 1,600
- Operating Systems: Microsoft Windows 2008 R2
- Applications: Microsoft Exchange, among others

BUSINESS VALUE AND TECHNICAL BENEFITS

- Defined and introduced universal policies for data loss prevention across the hospital
- Lowered proliferation of confidential healthcare data across the NHS Trust
- Identified broken business processes transmitting confidential data
- Monitored and protected communications of sensitive content to public websites
- Ensured patient records are protected and that the hospital is not exposed to fiscal penalties from ICO

"The health service holds some of the most sensitive information available. The damage and distress caused by the loss of a patient's medical record is obvious, therefore it is vital that organizations across this sector make sure their data protection practices are adequate."

Dawn Monaghan
Strategic Liaison Group Manager
for Public Services
Information Commissioner's Office

Starting with email monitoring

The goals for the first phase of the deployment are to further understand confidential data flows, and address the issue through enhancement of a data security education program. The hospital will begin by monitoring email communications to passively inspect network traffic for confidential data that is being sent in violation of security policy. This will help the team to understand how confidential data is being used, whether the user is on or off the corporate network, and gain enterprise visibility.

In due course, Data Loss Prevention will be expanded across the entire spectrum of information risk and compliance needs. This includes finding confidential data wherever it is stored, creating an inventory of sensitive data, and automatically managing data cleanup (discovery). It will be used to automatically enforce security policies to proactively secure data and prevent confidential data from leaving the Trust (protection). And it will be used to define universal policies across the hospital, remediate and report on incidents, and detect content accurately within one unified platform (manage).

Mobile monitoring may also be introduced at a later stage. The hospital already has end-user PC device monitoring, and all laptops are encrypted. However, mobile monitoring will add an extra layer of confidence, monitoring outbound email and Web communications—and giving users the freedom to access apps and files from their mobile devices without putting sensitive data at risk.

"Data Loss Prevention gives the Bedford Hospital NHS Trust the visibility around confidential electronic data that is exposed whilst at rest within the trusts boundaries, as well as a clear understanding of how confidential information is being moved."

Mark Austin
CIO
Bedford Hospital NHS Trust