

# Case Study: Southend University Hospital NHS Foundation Trust



Southend University Hospital   
NHS Foundation Trust

## The Southend University Hospital NHS Foundation Trust stops patient data leaks with Proofpoint

### introduction

Southend University Hospital NHS Foundation Trust is one of the UK's key healthcare trusts. Established as a Foundation Trust since June 2006, the Trust prides itself on delivering a superb level of medical care and utilising best of breed technology to maintain services and communications with relevant parties.

With over 6000 IT users using roughly 2500 PCs, the IT department has a significant role to play in the day to day access to critical patient and medical data. The IT department services one of the largest hospitals in the Essex region and delivers IT services to a wide and varied number of satellite departments such as pharmacy as well as offering remote access to data for external GPs.

"As a department, we provide a lot of services across the Trust, not only within the hospital itself but also to personnel who work remotely...it's fair to say there are areas within the Trust that are so dependent on our IT systems, that they can't function without them," explains Konrad Hutchins, Acting 3rd Line Team Leader, Southend University Hospital NHS Foundation Trust.

The IT department consists of 50 staff including systems and project managers, developers, network technicians and first, second and third line support staff. The Trust hosts 170 servers hosting mainly Microsoft applications and bespoke clinical applications. The Trust also utilises a Citrix solution for remote access and application delivery. The data network is built on Cisco hardware.

"Proofpoint enabled us to strengthen the business case for outbound security. We were able to go the Governance department and illustrate the security risk to the Trust due to the amount of PII data that the Trust was moving around unsecured. This made the investment in Proofpoint a no-brainer."

Konrad Hutchins  
Acting 3rd Line Team Leader, Southend Univ Hospital

### Business challenge

"What we required was an email encryption solution that integrated easily into our current Exchange deployment as well as the back end IT infrastructure. The key benefits had to be that it was invisible to the end user and easy to deploy as well as being simple for the user and the recipient to use."

- Konrad Hutchins

### Proofpoint solution

Southend University selected the Proofpoint Messaging Security Gateway™ appliance to protect over 6000 employee mailboxes from offensive material and to protect data.

### Results achieved

With this project complete, Hutchins believes that Southend University Hospital NHS Foundation Trust has achieved its goal for both inbound and outbound mail security. In terms of future plans for Proofpoint, Hutchins concludes, "We're happy with Proofpoint, we wanted a solution that was future proof and robust and that's what we got. In the future we'll be developing upon the work that has been done, tweaking the system as the Trust requires. Email archiving may be the next project in terms of mail security but it's a while off."

### situation

In May 2008, the IT department became aware that the Trust needed to review and enhance its current levels of email security as a result of the stringent regulations regarding patient information and the movement of that information between necessary parties.

Southend University Hospital NHS Foundation Trust had already taken the strategic decision not to use NHS Mail so using this application to send and receive encrypted email was not an option. Instead their existing email environment centred on a deployment of Microsoft Exchange 2003 soon to upgrade to the 2007 version. In addition to Microsoft Exchange 2003, the Trust deployed a Barracuda email security solution to deal with spam. This would complement an existing Sophos deployment to deal with viruses.

According to Hutchins, the reason for not using NHS Mail was simple. Having invested and integrated Microsoft Exchange 2003 into a complex IT environment, the team felt that deploying NHS Mail would not give them the security they required to meet the exacting standards of governance regarding PII data. "In effect we would lose control of our data using NHS Mail and that was not a situation we wanted. What we quickly realised was that with NHS Mail, our users had to sign up for an NHS Mail account to send data securely, increasing administration and requiring a lot of user training and understanding to work effectively."

# Case Study: Southend University Hospital NHS Foundation Trust

## proof of concept

The Trust worked alongside Proofpoint partner NTS, in organising a 30-day “Proof of Concept” audit on outbound mail. The objective of the audit was to understand how much sensitive information, if any, could potentially leak from the Trust.

“We need to keep control of our data and know where it is going. Data loss is real issue for all NHS Trusts and its something we need to address. The audit provided the means of tracking data when liaising with other Trusts and third parties such as external GPs, social services and other organisations. Users could send an email that was automatically encrypted and the recipient had to come to us to retrieve the information securely” explained Hutchins.

What the IT team quickly realised during the audit was that the Proofpoint appliances could achieve end point security at the same time as providing anti-spam and anti-virus protection all within one system. They also realised that the Proofpoint solution would only require two appliances to give the Trust what they needed with room for expansion, as opposed to four Barracuda appliances currently in place.

“This was a key differentiator for Proofpoint. The Barracuda appliances were already creaking under the weight of inbound traffic whereas the Proofpoint appliances have plenty of room for expansion and can easily scale to the growing demands of the Trust’s

inbound and outbound mail. We decided on Proofpoint appliances as they were the best ones for the job.”

With technical support from both Proofpoint and NTS, Hutchins and his team were able to track any outbound data leaks from within the Trust. “We wanted to be able to lock down the PII. The results of the audit built the business case, not only for secure mail but also for the replacement of the Barracuda boxes as we

### Proofpoint Products Deployed

- Proofpoint Messaging Security Gateway
- Proofpoint Secure Messaging
- Proofpoint Regulatory Compliance
- Proofpoint Spam Detection
- Proofpoint Zero-Hour Anti-Virus
- Proofpoint Content Compliance
- Proofpoint Dynamic Reputation

found that the Proofpoint appliance was picking up spam and viruses that should have been identified by the Barracuda system.”

During the audit, the Proofpoint appliance highlighted over 1,000 instances of unsecure outbound mail containing pertinent information which should have been encrypted.

## benefits

Proofpoint’s ability to seamlessly integrate within the Trusts existing framework and deploy secure outbound mail to users “ticked all the boxes from the IT side of the business,” explained Hutchins. “The uptake from within the Trust has been both dramatic and organic. As word spread around the departments we saw requests to have the secure mail functionality coming from all areas of the Trust, especially the non-medical departments such as finance. This highlighted to the Board that the need for the Proofpoint solution expanded well beyond the clinical requirements and instead became a business requirement.”

“For us, the benefits of deploying Proofpoint have been exceptional. We’re now able to control our data and track where it is going. We’ve deployed a secure mail system which is simple and easy to use for everyone and we’ve reduced our ongoing costs with reduction of appliances yet increased our inbound and outbound mail protection and maintained user accessibility to vital data in a secure manner.”

By reducing the number of appliances by half and being able to combine inbound and outbound protection under one central management system, Southend University Hospital NHS Foundation Trust has been able to re-direct IT resource into other projects such as USB and laptop data encryption.

Throughout the audit, the project team had the full support of both Proofpoint and NTS. Whenever necessary they were able to utilise and call upon the skills within NTS and Proofpoint to iron out snags and answer questions, thus making it easier and quicker for the department to become self sufficient in maintaining the Proofpoint solution once deployed. ➡

## About Southend University Hospital NHS Foundation Trust

Southend University Hospital NHS Foundation Trust is one of the UK’s key healthcare trusts. Established as a Foundation Trust since June 2006, the Trust prides itself on delivering a superb level of medical care and utilising best of breed technology to maintain services and communications with relevant parties.

## About Proofpoint, Inc.

Proofpoint secures and improves enterprise email infrastructure with solutions for email security, archiving, encryption and data loss prevention. Proofpoint solutions defend against spam and viruses, prevent leaks of confidential and private information, encrypt sensitive emails and archive messages for retention, e-discovery and easier mailbox management. Proofpoint solutions can be deployed on-demand (SaaS), on-premises (appliance) or in a hybrid architecture for maximum flexibility and scalability.

©2009 Proofpoint, Inc. All rights reserved. Proofpoint, Proofpoint Protection Server, Proofpoint Messaging Security Gateway, Proofpoint Virus Protection, MLX, MLX Engine, and Dynamic Update Service are trademarks of Proofpoint, Inc. Product and company names listed are trademarks or trade names of their respective companies. 3/09