

# Case Study

## Dorset County Hospital NHS Foundation Trust

### Dorset County Hospital install fully integrated email encryption solution to comply with government policy

**“The Cisco IronPort Solution has allowed us to meet Connecting for Health policy and ensures that all information in transit is secure. The increased inter-connectivity between other trusts in the region has allowed the hospital to provide a higher level of service to our users .”**

**Brian Stalker, IT Manager, Dorset County Hospital**

#### Company Background

Dorset County Hospital was established in 1991 as part of a long-term project to bring together all the local services for acutely ill patients onto one hospital site. The new hospital was completed in 1997, and then more recently, awarded Foundation Trust status in June 2007.

Dorset County Hospital are the main provider of acute hospital services to a population of around 210,000, living within Weymouth and Portland, West Dorset, North Dorset and Purbeck. The Trust also provides renal services for patients throughout Dorset and South Somerset; a total population of 850,000.

Their vision for the future is ambitious and by 2010 aim to be one of the most highly regarded, pioneering NHS healthcare providers in the UK; to be judged on results and the quality of care that is provided to those who choose to use their services.

#### The Challenge

Recent media coverage surrounding high profile security breaches within public sector organisations has led to an increasing amount of pressure placed upon NHS organisations to protect confidential patient and staff information. In December 2007, Connecting for Health Legislation was imposed, forcing the NHS to address the growing issues surrounding data leakage and therefore implement rigorous measures to minimise potential risk.

A security project at the hospital would be large scale, affecting approximately 2500 users and connecting to five other regional trusts within the Strategic Health Authority along with external agencies. Potential options to overcome the security challenge were limited. Impending legislation meant a 'do-nothing' approach was not an option and limited resource would delay an in-house implementation.

Aside from government compliance, the challenge also called for the chosen technology to be implemented whilst maintaining full user operations, with little or no impact on business efficiency. Compared to the three other competitive technologies, the chosen IronPort solution was the most cost effective and also the most user friendly. The Cisco IronPort solution is compliant with regulation and meets Connecting for Health guidelines. The solution is fully interoperable with the N3 network allowing the hospital to connect to other trusts within the Strategic Health Authority.

ANS Group and Dorset County Hospital have collaborated together on previous successful projects. With over 12 years experience providing innovative and value added solutions to the public sector, and specialist security expertise with Cisco and IronPort, ANS came highly recommended from IronPort as a preferred strategic solutions provider.





# Case Study

## The Solution

The solution was based around three encryption mechanisms;

- **Transport Layer Security (TLS)** – Automated Gateway to Gateway encryption - No dependency on the sender or recipient to encrypt or decrypt the e-mail.
- **Cisco IronPort PXE** - Standards based Gateway to Endpoint encryption - Eliminates legacy PKI complexity and can be opened by the intended recipient regardless of location or mail client.
- **PGP** – Standards based Gateway to Endpoint PKI encryption, managed at the Gateway – Automated encryption and decryption without user interaction.

Dual Cisco IronPort C360 Email security appliances were deployed at each site (7 sites in total) with TLS configured on a per domain destination. When a user sends a mail to a recipient at another trusted site, the Cisco IronPort appliance negotiates a TLS connection to the destination Cisco IronPort appliance and sends the message over a TLS encrypted tunnel. As the solution has been integrated with the neighbouring Somerset NHS organisation, there are just less than 200 domains secured in this way.

For recipient domains not covered by TLS or domains outside of the NHS PXE, encryption has been configured via intelligent content filters. End users can be given the option to encrypt email on demand from their mail client without the use of extra software. The recipient receives a notification e-mail and is directed to double-click on the "PXE Secure Envelope" to start the decryption process through a web browser. The recipient is prompted to enter their login credentials, authenticating that they are the intended recipient. When the user is validated by the Cisco Registered Envelope System, the per-message key is automatically sent to the browser, and the message is decrypted and displayed to the recipient.

For specific domains that require encryption for all mails, but where a direct TLS connection is not possible, automatic PGP encryption and decryption is provided via a Cisco IronPort Encryption Appliance (IEA). Each Cisco IronPort C-series appliance is configured to route mail from the trust gateway via TLS to the IEA. Mails are then encrypted or decrypted as required and sent back to the C Series appliance for delivery.

End users within Dorset NHS are not required to use any keys or software locally as these are hosted centrally on the IEA and all routing is configured on the C-Series appliance on a per-sender or recipient domain basis.

The specific network design and mail policies were derived through close consultation between ANS and each trust to ensure the right functionality was delivered. A number of Smart Filters have been developed by ANS with the help of IT staff from the trusts so that confidential information such as NHS numbers and specific hospital identifiers can be used to trigger PXE Encryption in order to protect patient data.

The six Trusts covered by the system are; Dorset County Hospital NHS Foundation Trust, Dorset PCT, Bournemouth and Poole PCT, Poole Hospital NHS Trust, Royal Bournemouth and Christchurch NHS Foundation Trust and Dorset Healthcare NHS Foundation Trust. These six trusts are now linked up to the Somerset network, which has also implemented the solution.

## The Business Benefits

**Seamless Integration** - ANS integrated the solution into the network efficiently and seamlessly without impacting end-users, ensuring there was no disruption to business efficiency.

**Compliance** - The Trusts are now fully compliant with the government's requirements for information governance, ensuring complete confidentiality for patient and staff information.

**Simplicity** - As the appliances are on site at each trust, the solution is easy to maintain and manage. Year on year renewal of the Cisco IronPort licenses is also a very simple process.

**Data Security** - Now the solution is in place, Dorset County Hospital's network is free from risk of data loss, ensuring all information in transit is secure whilst remaining transparent to the end-user.

**Flexibility** - The solution is fully integrated into the Trusts' networks, meaning that the solution is scalable and can grow along with the hospital in the future.

**Secure Connection** - Cisco IronPort's technology also allowed for the hospital to connect to Somerset NHS, exceeding original expectations as some difficulties were anticipated here.

