

## A Huge Security Challenge for Health Trusts

With 60 years of protecting the health of citizens across the country, the NHS has seen many challenges, not least in the technology area, where the ability to share sensitive, private, personally identifiable data (PID) such as medical notes, x-rays and other patient data has become commonplace, opening up the need to protect this sensitive information wherever it travels.

David Nicholson, NHS Chief Executive, has directed that there should be no transfers of unencrypted personally identifiable data held in electronic format across the NHS. This default position ensures that patient and staff personal data are protected. Any data stored on a PC or other removable device in a non-secure area or on a portable device such as a laptop, PDA or mobile phone should also be encrypted. This is also now a requirement across all public sector organizations set by the Cabinet Secretary.

Protecting data comprehensively means protecting data in databases and applications, protecting files and documents and protecting information travelling via email. Voltage Security and its partners provide integrated solutions that address these areas.

## Voltage SecureMail – Easy to use encryption

Voltage SecureMail is the easiest to use email encryption solution – currently in use within multiple NHS Trusts and teaching hospitals as well as in large public and private healthcare systems around the world.

Voltage SecureMail is easy to implement and provides multiple levels of integration with your environment. You can choose to implement it as a service via the Voltage Security Network, as an on premise solution – which may be fully integrated with DLP solutions such as Proofpoint, or as a hybrid – where full integration with DLP solutions is available combined with access to the service to make configuration and ongoing operations extremely straightforward.

Voltage SecureMail is fully compatible with older email encryption approaches such as OpenPGP and S/MIME.

Voltage SecureMail is now used in the world's largest email encryption implementation of over 600,000 internal users and can be deployed at a fraction of the cost of other solutions.

For more information about Voltage SecureMail please visit: [www.voltage.com/nhs](http://www.voltage.com/nhs)

## Challenge Summary

Key reasons for the encryption within the NHS include:

- Complete protection of sensitive data, such as patient information
- Minimising the risk of data loss or misuse from outside of the network
- Minimising the risk of data loss or misuse from within the network
- Protection of individual and organisational reputation
- Achieve policy compliance
- Protection from litigation

## Benefit Summary

- Ability to define policies and check encrypted content
- Adhoc ability to send encrypted email to non NHSmail users
- Integration capabilities for mobile phone and Blackberry users
- Secure archiving capabilities to achieve current legal requirements
- Supports common email standards such as IBE, OpenPGP and S/MIME
- Available as on premise, SaaS and hybrid solution for easy integration

---

"Deploying Voltage email encryption is win-win situation for us: end users get an exceptional experience and administrators don't have to manage encryption keys, software downloads or installation of files,"

**IT Project Manager, NHS Teaching Hospital**



Frequently Asked Questions	NHSmail	Voltage
Can Patient Identifiable Data be sent via the system	<b>NO</b>	<b>YES</b>
Can a user use their own email address and email client	<b>NO.</b> A separate email account has to be set to use so multiple account to manage	<b>YES</b>
Ad-hoc encryption to anyone inside and outside of the NHS	<b>NO.</b> NHS Mail users can only send messages to other NHS Mail users	<b>YES</b>
Complete message control by only sender and recipient	<b>NO</b>	<b>YES</b>
Enforce Encryption of communication between NHS Mail users and external users	<b>NO.</b> Not without setting external party up with an NHS Mail account	<b>YES</b>
On-demand key generation for encryption	<b>NO</b>	<b>YES</b>
Can users force encryption at the desktop	<b>NO</b>	<b>YES</b>
Are messages stored anywhere outside of users Mail box	<b>NO</b>	<b>YES</b>
Can system integrate with internal Archiving system	<b>NO</b>	<b>YES</b>
Enforce policy at client to encrypt	<b>NO</b>	<b>YES</b>
Enforce policy at the gateway to encrypt based on potential content	<b>NO</b>	<b>YES</b>
Can external parties authenticate and read email from anywhere	<b>NO</b>	<b>YES</b>
Force encryption if a message has been previous encrypted	<b>NO</b>	<b>YES</b>
Support for AES 256, 3DES, DSA, SSL, PKCS#7 (S/MIME)	<b>NO.</b> AES 128 only	<b>YES</b>
Support for Common Criteria Certification	<b>NO</b>	<b>YES.</b> EAL-2 certification
Support for FIPS 140-2 certification	<b>NO</b>	<b>YES.</b> Part of toolkit
Allow compliance checks to be carried out on email for AV, Spam, content, etc (both inbound and outbound)	<b>NO</b>	<b>YES</b>
Allow use of group keys for encryption	<b>NO</b>	<b>YES</b>