

**Patient guidance leaflet for NHSMail**

****Corresponding and Sending Medical Information

by Email using NHSmail encryption service

**Introduction**

Salisbury NHS Foundation Trust is committed to improving communication with patients in a manner which supports their continued care.

Many patients now ask Clinicians and administrative staff to correspond via email to help them manage their health care needs. The Trust supports this, but has a legal duty to inform patients of the risks associated with email correspondence containing personal and health care information. At the same time the Trust is continually looking at the ways and means to reduce such risks.

Staff at Salisbury District Hospital now uses nhs.net accounts, however information sent from these to a non-nhs.net account are not considered a totally secure means when used to communicate with patients by email. For example your personal information could be read by other family members or friends who have access to your email account, or if you are using a work email account, your employer may have access to these emails, which may then be stored on your employer’s system. In rare circumstances, your personal information will be open to access by malicious or criminal cyber products that have the ability to intercept emails without authority.

NHSmail has an encryption facility which is considered a far more secure means for emailing patients when personal or sensitive information is involved. As such this would be the preferred means to communicate with patients who wish to correspond by email. You are able to easily identify NHS mail emails which end with @nhs.net.

This leaflet provides guidance for patients who are recipients of encrypted emails sent from an NHS mail accounts. It explains how to register with the service and to subsequently open and read an encrypted email and send an encrypted reply.

**NHS Mail encryption feature**

A facility provided as part of NHSmail includes an encryption feature that allows Trust to exchange information securely with patients through their normal email browser accounts which would not otherwise be considered a secure means. This enables the Trust, when using NHS Mail encryption service, to communicate securely and easily with individuals of ANY email service without having to manually encrypt sensitive information.

Once a message is sent from NHSmail, using this service, it is encrypted and protected with a digital signature to assure the recipient that the message is authentic and has not been forged or tampered with. Formatting of the message is preserved and attachments can be included.

**Other important considerations**

Whilst there are significant benefits for using this service for email communication with patients there are matters that need to be considered. In particular:

* Your consent as a patient to communicate with you by email will be required and if provided will be recorded in your records.
* There will be arrangements for opting-out of receiving information by email, should you wish to do so in the future, and this will be explained when signing-up to the service.
* You must contact the hospital if you change your email address.
* A review of the information requested will be carried out and the clinician/Trust reserves the right to refuse to email information if deemed inappropriate or sensitive.
* You need to be aware that message tracking (e.g. delivery or read receipts) is not available on encrypted emails.
* As the service sends and receives email over the Internet there are no guarantees that a message will reach you. Equally there is no guarantee on how quickly the message will be received.
* There are a number of attachment types which aren’t permitted to be sent via NHSmail, these include .exe files.

**The steps involved to set up**

Before being able to correspond with patients by email using the NHS mail encryption service there are two relatively simple steps involved which are:

* Obtaining your consent
* Registration and verification

**a. Patient Consent**

Firstly, you are asked to read carefully the Patient Consent to Communicate Medical information be Encrypted Email form. If you are happy to go ahead then you are asked to complete the Consent Form below and to return the original to the hospital. This form will be kept in your medical record for future reference.

Please remember to notify us if your email is changed or if you subsequently decide to opt-out of the service of receiving information by email.

**b. Registration and Verification**

Secondly, once the Consent Form is received you will be sent an initial encrypted email containing no personal or sensitive data and will contain a link to access the encrypted message. The message will look similar to this:

**Consent to communicate medical information by email**

**Patient Details:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| **First name:** |  | **Date of Birth** |  |  |
| **Surname:** |  | **NHS Number** |  |  |
|  |  | **Hospital Number** |  |  |
|  |  |  |  |  |
| **Address** |  | **Email Address:** |  |  |
|  |  |  |  |  |
|  |  | **Telephone No:** |  |  |
|  |  |  |  |  |
| **Town** |  |  |  |  |
| **County** |  |  |  |  |
| **Post Code** |  |  |  |  |
|  |  |  |  |  |

**Risks & Responsibilities:**

Unless using the NHS mail encrypted email facility then there are the following risks:

* Any information transferred out of the Trust’s network is NOT SECURE unless it is sent to e.g nhs.net, police.pnn, gcsx.gov.uk
* Your personal information could be intercepted by others who have access to your email account.
* If you are using a work email account, your employer may have access to these emails.
* Your personal information could be open to access by malicious or criminal cyber products that have the ability to intercept emails without authority.
* The Trust cannot be held responsible for the security of your personal information coming into and going out of our network.
* There is no guarantee that the information sent has not been changed before receipt.
* Your personal information will not be encrypted or sent in a locked file format.
* It is your responsibility to inform the Trust if your email addresses changes.

These risks would be mitigated if the NHS mail encryption facility is used.

It is your responsibility to look after any sensitive information sent to you. If you wish to keep any received emails it is recommend that you download them and store them safely as required.

**Trust Assurance:**

* A review of the information requested will be carried out and the clinician/Trust reserves the right to refuse to email information if deemed inappropriate or sensitive.
* A copy of any information sent or received will be retained in your medical records unless you specifically request otherwise by letter.
* Information will only be sent from an NHS network email – the address will end with @nhs.net.
* If registering with the NHS mail encrypted email service then encrypted emails will only be sent via email addresses ending @nhs.net.

By signing this document you accept and agree to the following statement:

**I agree that Salisbury NHS Foundation Trust can send confidential personal information including medical information to me via the email address I have provided. I have read and understood the risks associated with this, as detailed above and have been provided with a copy of the leaflet entitled: Patient Guidance: Corresponding and Sending Medical Information by Email using NHSmail encryption service.**

I wish information this information to be sent via (tick as appropriate):

a. Standard email (i.e. not encrypted) 

or,

b. NHS mail encrypted 

Signature:.........................................................................................

Date:........................