NHSmail Acceptable Use Policy

1. About this document

This document explains how the NHSmail service should be used. It is your responsibility to ensure that you understand and comply with this policy. It ensures that:

1.1. You understand your responsibilities and what constitutes abuse of the service

1.2. Computers and personal data are not put at risk

If you have any questions about these terms and conditions, you should contact the NHSmail team at: feedback@nhs.net

The NHSmail team reserves the right to update this document as necessary. A copy of the current version can be found at: http://www.nhs.net. Click 'Search Directory' and the Acceptable Use Policy (AUP) can be seen in the bottom left hand corner of the screen. (An NHS/N3 connection must be used).

Supporting information can be found via the NHSmail Training and Guidance pages at https://web.nhs.net/portal/InformationGuidanceServices/DefaultPage.aspx when logged into your account.

2. General information about the NHSmail service

2.1. The NHSmail service has been provided to aid the provision of health and social care and this should be your main use of the service. There may be circumstances under which it is necessary for a designated and authorised person other than yourself to view the contents of your files and folders within NHSmail, for example if you have a secretary or PA that organises your diary

2.2. If you are a member of clinical staff you may use the NHSmail service in relation to the treatment of private patients in accordance with your own professional codes of conduct

2.3. NHS staff contact details are provided in the NHS Directory to support the delivery of healthcare - these details will be shared across the NHS

2.4. All data retained within the service remains the property of the NHS

2.5. NHSmail accounts are owned by NHS Connecting for Health on behalf of the Secretary of State for Health and provided to NHS staff for their use

2.6. The NHSmail programme reserves the right to withdraw an email account from use should operational requirements dictate

3. Your responsibilities when using the service

3.1. General responsibilities:

3.1.1. You must not use the NHSmail service to violate any laws or regulations of the United Kingdom or other countries. Use of the service for illegal activity is usually grounds for

immediate dismissal and any illegal activity will be reported to the police. Illegal activity includes, but is not limited to, sending or receiving material related to paedophilia, terrorism, incitement to racial harassment, stalking and sexual harassment and treason. Use of the service for illegal activity will result in the immediate suspension of your NHSmail account

3.1.2. You must not use the NHSmail service for commercial gain. This includes, but is not limited to: unsolicited marketing, advertising and selling goods or services

3.1.3. You must not attempt to interfere with the technical components, both hardware and software, of the NHSmail system in any way

3.1.4. When you set up your NHSmail account you must identify yourself honestly, accurately and completely

3.1.5. You must ensure your password and answers to your security questions for the NHSmail system are kept confidential and secure at all times. You should notify your Local Organisation Administrator (LOA) if you become aware of any unauthorised access to your NHSmail account. You should never input your NHSmail password into any other website other than www.nhs.net. You will never be asked for your NHSmail password. E.g. by phone or email. Do not divulge this information to anyone, even if asked.

3.1.6. Email messages are increasingly a source of viruses which often sit within attached documents. NHSmail is protected by anti-virus software although occasionally, as with any email service, a new virus may not be immediately detected. If you are unsure of the source of an email or attachment you should leave it unopened and inform your local IT services. You must not introduce or forward any virus or any other computer programme that may cause damage to NHS computers or systems. If you are found to be deliberately responsible for introducing or forwarding a programme that causes any loss of service, NHS Connecting for Health may seek financial reparation from your employing organisation

3.1.7. You must not use the NHSmail service to disable or overload any computer system or network. Where excessive account activity is detected your account could be suspended without notice to safeguard the service for all other users

3.1.8. All communication you send through the NHSmail service is assumed to be official correspondence from you acting in your official capacity on behalf of your Organisation. Should you need to, by exception, send communication of a personal nature you must clearly state that your message is a personal message and not sent in your official capacity

3.1.9. You must familiarise yourself with the NHSmail Training and Guidance pages which include important policy guidelines, information about known issues with the service and user/administration guides

3.1.10. If you are accessing your NHSmail account from a non-NHS device (i.e. a home computer, personally owned laptop or in an internet cafe) you should only access the service via the web at www.nhs.net and not through an email programme such as Microsoft Outlook unless you have explicit permission from your own organisation to do so

3.2. Responsibilities when using the NHSmail email service:

3.2.1. You must not attempt to disguise your identity or your sending address

3.2.2. You must not send any material by email that could cause distress or offence to another user. You must not send any material that is obscene, sexually explicit or pornographic. If you need to transmit sexually explicit material for a valid clinical reason then you must obtain permission from your local Caldicott Guardian. [Note: GPs may need to refer to the Caldicott Guardian at their local PCT]

3.2.3. You must not use the NHSmail service to harass other users or groups by sending persistent emails to individuals or distribution lists

3.2.4. You must not forward chain emails or other frivolous material to individuals or distribution lists

3.2.5. It is your responsibility to check that you are sending email to the correct recipient, as there may be more than one person with the same name using the service. Always check that you have the correct email address for the person you wish to send to - this can be done by checking their entry in the NHS Directory

3.2.6. Email is admissible as evidence in a court of law and messages can be classified as legal documents. Internal emails may also need to be disclosed under the Freedom of Information Act 2000 and the Data Protection Act 1988. Emails should be treated like any other clinical communication and care should be taken to ensure that content is accurate and the tone is appropriate

3.2.7. Use of the NHSmail SMS/Fax feature is for NHS business use only to support the delivery of Health and social care.

3.3. Responsibilities when using the NHS Directory service:

3.3.1. It is your responsibility to make sure that your details in the NHS Directory are correct and up to date

3.3.2. You must not use the NHS Directory to identify individuals or groups of individuals to target for commercial gain, either on your behalf or on that of a third party

3.4. Information governance issues

3.4.1. The General Medical Council (GMC) Good Medical Practice guidance requires doctors to keep clear, accurate and legible records. It is important that emails do not hinder this. You should ensure that relevant data contained in emails is immediately attached to the patient record. Failure to do so could have implications on patient safety

3.4.2. NHSmail supports the secure exchange of information and is not designed as a document management system. Documents or emails that are required for retention/compliance purposes should be stored within your organisation’s document management system in accordance with local Information Governance policies

3.4.3 Your Organisation is entitled to seek access to the contents of your mailbox, sent/received messages or other audit data as required to support information governance processes without your prior consent. Such requests are strictly regulated with the process detailed in the training and guidance pages

4. Using NHSmail to exchange sensitive information

4.1. The NHSmail service is a secure service, this means that NHSmail is authorised for sending sensitive information, such as clinical data, between NHSmail and:

NHSmail addresses (i.e. from an '*.nhs.net' account to an '*.nhs.net' account),

Government secure email domains (between *.nhs.net and *.gsi.gov.uk, *.gse.gov.uk and *.gsx.gov.uk),

Police National Network/Criminal Justice Services secure email domains (between *.nhs.net and *.pnn.police.uk, *.scn.gov.uk, *.cjsm.net),

Ministry of Defence secure email domains (*.nhs.net and *.mod.uk),

Local Government/Social Services secure email domains (*.nhs.net and *.gcsx.gov.uk).

If you intend to use the service to exchange sensitive information you should adhere to the following guidelines:

4.1.1. You should make sure that any exchange of sensitive information is part of an agreed process. This means that both those sending and receiving the information know what is to be sent, what it is for and have agreed how the information will be treated

4.1.2. Caldicott and local Information Governance principles should apply whenever sensitive information is exchanged

4.1.3. As with printed information, care should be taken that sensitive or personal information is not left anywhere that it can be accessed by other people, e.g. on a public computer without password protection

4.1.4. When you are sending sensitive information you should always request a delivery and read receipt so that you can be sure the information has been received safely. This is especially important for time-sensitive information such as referrals

4.1.5. You must not hold sensitive or personal data in your calendar if your calendar may be accessed by other people who are not involved in the care of that person

4.1.6. If personal identifiable information is visible to other people it is your responsibility to make sure that those people have a valid relationship with the person

4.1.7. You must always be sure that you have the correct contact details for the person (or group) that you are sending the information to. This is especially important if you are sending information using the fax or SMS services. If in doubt you should check the contact details in the NHS Directory

4.1.8. You may only use the NHSmail service for patient referrals if Choose and Book has not yet been implemented in your organisation; the Choose and Book service is unavailable to you for some reason, or the service you need to refer to is not available via Choose and Book

4.1.9. If it is likely that you may be sent personal and/or sensitive information you must make sure that the data is protected. You should only access your account from secure, encrypted devices which are password protected and unattended devices must be locked to ensure that data is protected in the event of the device being lost or stolen

4.1.10. If using SMS as an alerting or notification system you should ensure you have carried out a relevant risk assessment in relation to the limitation of SMS, particularly its insecure nature and lack of delivery guarantee and delivery notifications. It is not recommended for use where personal data is exchanged or guaranteed delivery is required

4.1.11. Remember that personal information is accessible to the data subject i.e. the patient, under Data Protection legislation

Published: 29th May 2012