CODE AND PRACTICE FOR CONNECTION of COMMUNITY PHARMACIES TO NHSNet SCOTLAND

Source: ISSG, ISD

Date Released: 6 January 2004

Version: 1.36

CODE AND PRACTICE FOR CONNECTION of PHARMACIES TO NHSNet

Introduction

This Code and Practice for connection of pharmacies to NHSnet has been written to facilitate and ensure acceptable use of NHSnet by Pharmacist organisations in Scotland.

Aims of NHSnet

1. NHSNet aims to provide the best possible network services to its customers in terms of quality, access, security, reliability and value for money to support patient care and administration in the NHS.

Background and Definitions

1. "*NHSnet*" is the name given to the networking services and facilities that support the communication requirements of the National Health Service (NHS).

2. Information Systems Support Group (ISSG) is responsible for the provision of *NHSnet* in Scotland. ISSG will resolve any dispute over the interpretation of this Policy. ISSG takes responsibility for Scottish users of *NHSnet,* and researches, develops and provides advanced electronic communication facilities for use within the NHS Scotland community.

3. This Policy applies to any person lawfully running a retail pharmacy business, who provides NHS pharmaceutical service under the NHS Act 1977 (or the equivalent) and who is a User Organisation for the purposes of NHSNet.

4. Such a User Organisation may only permit the use of NHSnet within its organisation by an individual included in the Royal Pharmaceutical Society of Great Britain register of pharmaceutical chemists or by an individual working under that person's direct supervision.

5. It is the responsibility of the User Organisation to ensure that members of their own user community use NHSnet services in accordance with the current Acceptable Use Policy (AUP) and current legislation, technical and security requirements.

6. For the purposes of this Code and Practice a User Organisation is defined as a Community Pharmacy in which a connection to NHSnet is terminated.

Policy Documents making up the Code of Connection

1. Acceptable Use Policy
2. Security Policy
3. Declaration

Availability

Further copies of these documents may be obtained from ISSG (see Annex A).

Disclaimer

ISSG cannot accept any liability for loss or damage resulting from the use of the material contained herein. The information is believed to be correct but no liability can be accepted for any inaccuracies.

NHSnet - Acceptable Use Policy

Contents

Why an Acceptable Use Policy?

The purpose of this Acceptable Use Policy (AUP) is to guide users to use NHSNet connected facilities responsibly. That will assist the NHSNet Network managers to protect the integrity of the network so that at all times it will be available to serve your needs, those of patients, and of other users.

NHSnet will be used exclusively to enhance the quality of patient care, or to facilitate administration in the Health Service and the professional work of those providing the care.

The consequences of failing to observe this policy are potentially very serious, and the Compliance section sets out the range of measures that exist to enforce this Policy.

As the *NHSnet* is a closed network and access from other networks is very strictly controlled, users should be aware that the greatest risk to security is posed by those within the network, and not by outsiders. While the AUP can contribute to an enhanced level of security, as compared to that found in an unregulated network, this is dependent on all users observing the basic rules. Users should remember that *NHSnet* cannot protect their systems from the actions, legitimate or otherwise, of other users. Therefore, an additional written and enforceable Security Policy has become essential. A thorough understanding of the Security Policy document and of professional guidance on protecting the privacy and security of clinical data is essential. You should also check that you meet the requirements of the Data Protection Acts 1998 and that you behave in accordance with the law as it applies to the relevant part of the UK, at all times.

Please read this AUP document carefully and ask ISSG if you have any questions (see Annex A).

Acceptable Use

A User Organisation may use *NHSnet* for the purpose of interworking with other User Organisations, and with organisations attached to networks that are reachable via interworking agreements operated by *NHSnet*. All use of *NHSnet* is subject to payment of the appropriate charges in force during the period of service.

NHSnet may be used for any normal NHS business activity that is in furtherance of the aims and policies of the NHS.

NHSnet may not be used for any of the uses outlined in the Unacceptable Use section below.

User Organisations must have documented arrangements in place to ensure that measures outlined in the Security Policy document are adhered to.

Unacceptable Use

NHSnet may NOT be used for any of the following:

1. The creation or transmission (other than for properly supervised and lawful clinical purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;

2. The creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety;

3. The creation or transmission of defamatory material;

4. The transmission or obtaining of material such that this infringes the copyright of another person;

5. The transmission of unsolicited commercial or advertising material either to other User Organisations, or to organisations connected to other networks;

6. Non-Healthcare activity which may grossly abuse the service;

7. Other activities that do not benefit patient care or that do not support the professional concerns of those providing that care, where those activities constitute gross abuse of the service;

8. Gross abuse of the service by the unsolicited sending of inappropriate e-mail to large numbers of people, whether on *NHSnet* or on the Internet.

9. Deliberate unauthorised access to facilities or services accessible via *NHSnet*;

10. Deliberate activities with any of the following characteristics:

    - flagrant wasting of staff effort or networked resources, including time on end systems accessible via *NHSnet* and the effort of staff involved in the support of those systems;
    - corrupting or destroying other users' data;
    - violating the privacy of other users;
    - disrupting the work of other users;
    - using *NHSnet* in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
    - continuing to use an item of networking software or hardware after ISSG has requested that use cease because it is causing disruption to the correct functioning of *NHSnet*;
    - other misuse of *NHSnet* or networked resources, such as the introduction of "viruses".
    - Where *NHSnet* is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of *NHSnet*.
    - Introduction of Wireless LAN connections or products using WLAN technology.

11. Note that this list is not exhaustive, and will be updated in the light of experience.

12. If you are in doubt about whether you may use *NHSnet* for a particular purpose, you should seek advice from ISSG (See Annex A).

13. It is not permitted to provide access to *NHSnet* by third parties.

Compliance

1. It is the responsibility of the User Organisation to take all reasonable steps to ensure compliance with the conditions set out in this AUP and to ensure that unacceptable use of *NHSnet* does not occur. The discharge of this responsibility must include informing those at the Organisation with access to *NHSnet* of their obligations in this respect and exercising logging and monitoring of user behaviour in accordance with the guidance set down by the Information Commissioner.

2. Connection may be subject to a satisfactory site visit by ISSG to verify compliance with the NHSnet security policy.

3. All changes to the connected environment must be communicated to ISSG prior to implementation.

4. The approval will be subject to annual review.

5. If ISSG have reason to believe that your Organisation's use of resources may contravene any principle in this AUP then ISSG reserve the right to instruct BT or CWC to terminate suspend the connection. When the issue has been remedied to the satisfaction of ISSG the connection will be restored.

6. Where violation of these conditions is illegal or unlawful, or results in loss or damage to *NHSnet* resources or the resources of third parties accessible via *NHSnet*, the NHS reserve the right to instigate an investigation and retain forensic evidence.

7. If you are given notice of any investigation into a security matter relating to a contravention of this AUP, you may appeal to ISSG giving the notice within 28 days of such notice being given.

8. It is preferable for misuse to be prevented by a combination of responsible attitudes to the use of *NHSnet* resources on the part of users and appropriate disciplinary measures taken by their Organisations.

9. If you should become aware that your staff or colleagues are breaching this AUP then you should report this to ISSG at once and address it within your own organisation, where appropriate.

NHSnet - Security Policy for Pharmacies

Introduction

Users should be aware that *NHSnet* cannot protect the data on their systems from the actions, legitimate or otherwise, of other network users. It is therefore your responsibility to protect data held within your Organisation from unauthorised access, whether from within your Organisation, or via the *NHSnet*, or any other network. Likewise the safety and privacy of clinical data being transmitted from one clinical domain to another needs to be protected to very high standards during transit. *NHSnet* services are authorised for your Organisation's use, **only registered pharmacists (or individuals directly supervised by them) authorised by you should be allowed access to *NHSnet***.

Security Policy

1. Data held within an Organisation needs to be protected from any unauthorised access. This should be undertaken in the following ways;

   a. Your system must have adequate staff identification and authentication controls, logging and monitoring to detect actual or attempted misuse.

   b. You must ensure that there is readily accessible and well-publicised documentation to support these identification and authentication controls. This document should clearly state that members of staff who fail to comply with the terms of the document will be liable to disciplinary action.

2. Person Identifiable clinical data that is transmitted over the *NHSnet* must be protected by cryptographic services conforming to current NHS standards at all times. It is ultimately the User Organisation who is responsible for any data transmitted.

3. You must protect the security and privacy of other Organisations attached to the *NHSnet* by the following means;

   a. Your Organisation must have a malicious software prevention policy in place and it must be implemented to accept scheduled updates from your vendor.

   b. All data/files which you send or receive over the *NHSnet*, or by any other means, must be scanned by an up to date virus scanner on your system, and the software for this will need to be updated periodically by mechanisms appropriate to your software.

   c. You must ensure you have clear, documented policies preventing your staff from using for illegitimate purposes, data that has been accessed via the *NHSnet* from other Organisations. This is regardless of whether the access is by legitimate or illegitimate means. Should this transgression occur, it would provide grounds for disciplinary action against the member(s) of staff involved.

4. You must notify ISSG of the existence of, or changes to, **concurrent connections via any dial-up service which enable stock ordering**.

5. All incidents that constitute a threat to *NHSnet* security must be reported to ISSG immediately.

6. You must ensure that physical access to the *NHSnet* router and ancillary equipment is restricted to only authorised personnel.

Pharmacist Declaration of Compliance with NHSnet Policies

A named pharmacist has to take responsibility for signing this document. If the pharmacy is not owned and managed personally by a pharmacist, this should be the pharmacist manager employed to manage the day-to-day operations of the pharmacy. A pharmacist manager will be signing both as an individual and on behalf of the owner of the pharmacy. The document should be countersigned by the person responsible for security if different to named pharmacist. Should you not understand any of it and if you do not have a member of staff who can explain the issues, then please consult ISSG.
This declaration will normally remain valid for a period of five years subject to satisfactory annual review. After that time, a fresh declaration should be signed. If the person signing this declaration ceases to remain as representative the new representative should sign a fresh declaration.

The representative signing this document has responsibility for making all new members of staff in the Community Pharmacy aware of the terms of this declaration and monitoring their compliance.

Please complete this form in capital letters and return to ISSG (see Annex A).

Name and Postal address of your organisation

Name of Pharmacy on Health Authority Pharmaceutical List.....

Health Authority .....

Trading Name.....

Address .....

.....

.....

Postcode .....

Person responsible for this declaration

Name.....

RPSGB registration number:.....

Telephone number Fax number .....

.....

Person responsible for security Name .....

Telephone number..... Fax number .....

.....

Please indicate the current method of stock ordering used in the Pharmacy:

Dial-up: Yes No Other

Name of main Pharmacy System Supplier.....

Declaration

I have read and understood and agree to comply with the ***NHSnet*** Acceptable use Policy and ***NHSnet*** Security Policy for Pharmacies.

Named Pharmacist:.....

Date.....

Countersignature of person responsible for security: .....

Date:.....

Contact Details for ISSG Annex A

Contact	Title	Telephone Number	Fax Number	Address
Ron MacDonald	Principal Communications Consultant	0131 551 8396	0131 551 8495	Trinity Park House South Trinity Road Edinburgh EH5 3SE
Alan Fleming	Pharmacy Infrastructure Programme Manager	0131 625 4310	0131 551 8495	
Phil Phillips	National Information Security Adviser	0131 551 8377	0131 551 8495	