CODE AND PRACTICE FOR CONNECTION OF DENTAL PRACTICES TO SWAN SCOTLAND

Source: NISG, NSS

Date Released: 01 June 2015

Version: 2.9

Location: http://www.psd.scot.nhs.uk/professionals/dental/edi.html

CODE AND PRACTICE FOR
CONNECTION OF DENTAL PRACTICES TO SWAN

Introduction

This Code and Practice for connection of dental practices to SWAN has been written to facilitate and ensure acceptable use of SWAN by dental practices in Scotland.

Aims of SWAN

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

2. National Services Scotland (NSS) is the common name for the Common Services Agency (CSA). Acting through its National Information Systems Group (NISG), NSS is responsible for the provision of SWAN in Scotland. NISG will resolve any dispute over the interpretation of this Policy. NISG oversees SWAN for Scottish users, and researches, develops and provides advanced electronic communication facilities for use within the NHS Scotland community.

3. This Policy applies to any person or legal entity lawfully running a dental practice, who provides NHS dental service under the NHS Act 1977 (or the equivalent) and who is a User Organisation for the purposes of SWAN and this Code and Practice, as defined below.

4. Such a User Organisation may only permit the use of SWAN within its organisation by an individual included in the General Dental Council register of dentists, or by an individual working under that person's direct supervision and for whom that person takes full responsibility for ensuring compliance with the obligations contained herein.

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

6. For the purposes of this Code and Practice a User Organisation is defined as a dental practice to which a connection to SWAN is provided under the terms of this Code and Practice.

Policy Documents making up the Code of Connection

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

Disclaimer

Neither NSS nor NISG accept any liability for loss or damage resulting from the use of the material contained herein or for any interruption to the service provided in facilitating access to SWAN. The information provided herein is believed to be correct but no liability can be accepted for any inaccuracies, or for the consequences of any interruption, suspension or termination of the service as described below.

SWAN - Acceptable Use Policy

Contents

Why an Acceptable Use Policy?

The purpose of this Acceptable Use Policy (AUP) is to guide users to use SWAN connected facilities responsibly. That will assist the SWAN 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.

SWAN is to 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 AUP are potentially very serious, and the Compliance section below sets out the range of measures that exist to enforce this AUP.

As the SWAN 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 SWAN cannot protect their systems from the actions, legitimate or otherwise, of other users. Therefore, an additional written and enforceable Security Policy is 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 are compliant with the law as it applies to the relevant part of the UK, at all times.

Please read this AUP document carefully and ask NISG if you have any questions (see Annex A for contact details).

Acceptable Use

A User Organisation may use SWAN for the purpose of interworking with other User Organisations, and with organisations attached to networks that can be contacted via interworking by agreement with NISG. All use of SWAN is subject to payment of the appropriate charges in force during the period of service.

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

SWAN may not be used for any purpose inconsistent with normal NHS business activity that is in furtherance of the aims and policies of the NHS, including those 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 below are adhered to.

Unacceptable Use

SWAN 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;

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

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

10. Deliberate activities with any of the following characteristics:

    - flagrant wasting of staff effort or networked resources, including time on end systems accessible via SWAN and the effort of staff involved in the support of those systems;
    - Altering, corrupting or destroying other users' data;
    - violating the privacy of other users;
    - disrupting the work of other users;
    - using SWAN 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 NISG has requested that such use cease because it is causing disruption to the correct functioning of SWAN;
    - other misuse of SWAN or networked resources, such as the introduction of "viruses".
    - Where SWAN is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of SWAN.
    - 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 SWAN for a particular purpose, you should seek advice from NISG (See Annex A).

13. It is not permitted to provide access to SWAN to 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 by all persons accessing the service via the User Organisation and to ensure that unacceptable use of SWAN does not occur. The discharge of this responsibility must include informing those at the User Organisation with access to SWAN 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 (further guidance is available on the Information Commissioner's website.)

2. Connection may be subject to a satisfactory site visit by NISG to verify compliance with the SWAN Security Policy outlined below. A site visit would involve a network audit to ensure that;-

    a. No other networks are connected other than SWAN
    b. Anti Virus software is installed, active and up to date on all networked devices.
    c. Internet Explorer (or other browser) has the correct Proxy settings.
    d. No unauthorised wireless networks are connected.

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

4. Approval of NISG to access SWAN will be subject to annual review.

5. NISG reserve the right to monitor the sites accessed by User Organisations via SWAN, and to retain such records of monitoring as are necessary in assessing compliance with this Code and Practice by any User Organisation. If NISG have reason to believe that a User Organisation's use of resources may contravene any principle described in the Code and Practice and AUP then NISG reserve the right to instruct BT or CWC or any other relevant service provider to terminate or suspend the connection. When the issue has been remedied to the satisfaction of NISG the connection will be restored.

   By signing the Dentist Declaration of Compliance below, User Organisations, including all employees or agents, waive any right to take any action against NSS or NISG or the NHS for losses suffered, whether directly or indirectly, as a result of any interruption, suspension or termination of access to SWAN.

6. Where an action by a User Organisation, or anyone for whom it accepts responsibility under this Code and Practice, in violation of these conditions constitutes a breach of the terms of this Code and Practice or an illegal or unlawful act, or results in loss or damage to SWAN resources or the resources of third parties accessible via SWAN, the NSS on behalf of 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 NISG giving the notice within 28 days of such notice being given. The parties shall take all reasonable steps in the circumstances to resolve any dispute amicably.

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

9. If you should become aware that your staff or colleagues are breaching the terms of this Code and Practice or the AUP then you should report this to NISG at once and address it within your own User Organisation, where appropriate.

SWAN - Security Policy for Dental Practices

Introduction

User Organisations should be aware that SWAN 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 SWAN, 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. SWAN services are authorised for your organisation's use ; **only registered dentists (or individuals directly supervised by them) authorised by you should be allowed access to SWAN**.

Security Policy

1. Data held within an organisation needs to be protected from any unauthorised access, and this is the responsibility of User Organisations, not NSS or NISG or the NHS. User Organisations should ensure protection in the following ways;

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

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

2. Personal Identifiable clinical data that is transmitted over the SWAN 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. User Organisations have a duty to protect the security and privacy of other organisations attached to the SWAN by the following means;

   a. An organisation must have a malicious software prevention policy in place and it must be implemented to accept scheduled updates from the vendor.

   b. All data/files which an organisation sends or receives over the SWAN, or by any other means, must be scanned by an up to date virus scanner on the User Organisation's system, and the software for this will need to be updated periodically by mechanisms appropriate to the relevant software.

   c. User Organisations must ensure they have clear and accessible documented policies and procedures which set out for staff their responsibilities and obligations with regards to the processing of personal and business data. Training should be provided to all staff to ensure that their knowledge is kept up to date. Registered dentists are required to follow their professional codes of practice.

   Where unauthorised access has occurred this may constitute grounds for disciplinary action against the member(s) of staff involved in accordance with the documentation provided by a User Organisation to its staff.

4. You must notify NISG 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 SWAN security must be reported to NISG immediately. **Notification of security alerts shall be submitted to nss.nationalsecurityadvisor@nhs.net**.

6. You must ensure that physical access to the SWAN router and ancillary equipment is restricted to only authorised personnel for whom you are responsible under the terms of this Code and Practice.

Remote Support

Contents

1) Introduction

Community Dental Practices may wish to engage with system suppliers to provide remote support. This type of support is generally provided by organisations using the accredited third party SWAN connection process; however some organisations choose to connect through the Internet. This is not a recommendation by NHS, NSS or NISG, but a request from Community Dental Practices and System Suppliers to allow this support using the SWAN infrastructure.

2) Risk Assessment

The use of remote access technology to provide remote support entails additional risks above previous normal operation that must be appropriately managed.

It is the responsibility of the Dental Practices as data controllers to manage these risks to protect the sensitive information that is held on dental practice systems.

Examples of heightened risks include the following:

- remote support engineer accesses personally identifiable, financial or other sensitive information for which they are not authorised (for example, browses through practice system or databases);
- remote support engineer damages practice systems or information stored on the systems (for example, by accidentally deleting data or reconfiguring aspects of the system incorrectly);
- vulnerabilities in remote support fourth party application are exploited by malicious code on the internet which spreads onto practice systems, potentially accessing/harvesting financial or other sensitive information, causing damage to practice systems and/or data and system downtime with associated subsequent cost to clean;
- member of staff in fourth party remote access application company (e.g. WebEx) 'overlooks' personal or sensitive information on a restricted remote desktop session or otherwise abuses privileges gained through administrative access to remote access server;
- internet user intercepts a remote session and accesses information for which they are not authorised.

The risks associated with the architecture are caused in particular by the use of a number of third party support organisations that have administrative access to practice machines. Dental Practices have limited and varying levels of control over the personnel and procedural controls within the support organisation.

It is anticipated that larger organisations will produce an appropriate risk management document detailing the impact and likelihood of each of these risks as part of a formal risk management process.

Smaller organisations that do not have the resources to devote to developing a full risk management document should undertake to implement the following controls:

- ensure the remote support session must be initiated by an individual at console in the practice and by no other means;
- establish a tight support contract for third party support organisations with clearly set out personnel and procedural controls e.g. record the names of all support engineers within their organisation that have access, get a signed acknowledgement from such employees that they acknowledged the importance of security of data and patient confidentiality and that breach of the rules will constitute a serious disciplinary matter;

- whenever possible ensure engineers providing remote support have undergone a Disclosure Scotland, basic check or other personnel screening equivalent process;
- limit the number of remote engineers to the minimum necessary, ideally named and identified individuals;
- select a single remote access technology, establish appropriate agreement with fourth party regarding use and configuration of this technology;
- limiting the number of third party support organisations to those that have agreed to the minimum set of controls;
- ensure all practice staff have appropriate security awareness training e.g. to be able to identify suspicious activity;
- system backup procedures are in place to recover from damage to practice data;
- separate data on practice system, store personally identifiable information in encrypted form that is not accessible by remote users.

3) Code of Practice Exception

Part 2 of attached Code of Practice document should be signed by a responsible site representative. The signatory will accept all risks (accidental or intentional) associated with this type of support. Some vulnerabilities have been identified above, but this is not a definitive list and will not identify all risks associated with this support arrangement.

- It is strongly recommended that the practice has a contract which is made or evidenced in writing, with the System Supplier for the remote support services. This should require the System Supplier to comply with obligations equivalent to those imposed on the practice by the Seventh Principle under the Data Protection Act 1998.

This agreement should clearly outline:

- that the supplier should act only on instructions from the practice;
- the guarantees in respect of the technical and organisational security measures they take;
- how the supplier takes all reasonable steps to ensure compliance with those measures; and
- any liability associated with the agreement.

It is important to note that the Seventh Principle relates to the security of the processing as a whole and the measures to be taken by data controllers to provide security against any breaches of the Act rather than just breaches of security.

To be returned to:
Customer Services
Dental & Ophthalmic Division
Gyle Square
1 South Gyle Crescent
Edinburgh
EH12 9EB

Dentist Declaration of Compliance with this Code and Practice and the SWAN Policies described within it.

Part 2 should only be completed by those dental practices engaging with suppliers to provide remote support services using the SWAN.

A named dentist has to take responsibility for signing this document. The document shall be signed by the dentist if the practice is run by an individual, by the partners if a partnership and by the director or company secretary if representing a dental company. Authorised signatories in the case of companies is permissible but evidence of authority must be provided e.g. board minute. The document should be countersigned by the person responsible for security if different to named signatory. Should the person signing not understand any part this agreement, then please consult NISG by email to nss.nationalsecurityadvisor@nhs.net.

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, NISG must be informed at least one month in advance and a new representative should sign a fresh declaration.

The representative signing this document has responsibility for making all members of staff in the practice(s) aware of the terms of this declaration, and for ensuring and monitoring their compliance. Please complete this form in capital letters.

Name and Postal address of your organisation

Name of practice/dentist on General Dental Council register of dentists ……

Health Authority ……..……

Trading Name ……

Address ……

Postcode ……

Person responsible for this declaration

Name ……

GDC registration number ……

Telephone number ……. Email ……

Person responsible for security Name

Telephone number ……. Email ……

Name of main Dental System Supplier ……

To be returned to:
Customer Services
Dental & Ophthalmic Division
Gyle Square
1 South Gyle Crescent
Edinburgh
EH12 9EB

Declaration – Part 1

I have read and understood and agree to comply with the foregoing Code and Practice containing the **SWAN** Acceptable use Policy and **SWAN** Security Policy for Dental Practices.

Named Dentist.....

Countersignature of person responsible for security.....

Date .....

Declaration – Part 2 (Remote support)

I have read the Remote Support information at page 7 and 8, agree to undertake a risk management exercise, and accept any risks associated with the Remote Support Services provided by:

System Suppliers legal & operating name……

Suppliers Name ……...

Person Responsible for this declaration ……..

Name……Signature……..

Date ……..