THIS DOCUMENT MUST BE READ AND AGREED BEFORE ANY ACCESS TO OR USE OF THE HSCN. IF YOU DO NOT AGREE TO ANY OF THE TERMS IN THIS DOCUMENT YOU ARE NOT AUTHORISED TO USE THE HSCN. ANY USE WITHOUT AUTHORISATION SHALL BE AT YOUR SOLE RISK. BY PROCEEDING WITH USE OF THE HSCN YOU AGREE TO THE TERMS SET OUT BELOW.

Introduction

Client as a commercial enterprise has requirements to be able to move data securely outside of the local IT environment. Standard public networks are not appropriate for the movement of confidential information, therefore Client requires a secure electronic environment with protection against intrusion from the internet and other health care providers, but which still allows connectivity to suppliers and other professional networks outside the NHS. Securnet was established in 2000 as a secure intranet for community pharmacy in the UK to facilitate these requirements and provide professional content as well as commercial services.

With the introduction of the NHS National Programme for IT, Securnet offered a set of connectivity services that combined with the core infrastructure, and satisfy the key criteria to allow community pharmacies to serve the NHS via N3 within the local community whilst protecting their current and future investment in ecommerce. N3 was subsequently superseded by Health and Social Care Network (HSCN). With the completion of HSCN compliance for Securnet – it is being made available to organisations outside of pharmacy who need to connect to HSCN.

Background and Definitions

"NHS Digital" means the Health and Social Care Information Centre, an executive non-departmental public body, whose head office is located at 1 Trevelyan Square, Boar Lane, Leeds, LS1 6AE.

"Securnet" is the name given to the underlying networking services and facilities provided by IQVIA that support the electronic communication requirements of independent contractors to the NHS in the UK such as, but not restricted to, pharmacy users.

"User Organisation" is a healthcare provider authorized to use Securnet for the purposes of connecting to the HSCN.

This Policy applies to any person employed by or working for a User Organization who is a client of IQVIA or otherwise has purchased access to the HSCN through Positive Solutions Limited ("PSL"), including, but not limited to, any individual lawfully running a retail pharmacy business, who provides NHS pharmaceutical service under the NHS Act 1977 (or the equivalent).

Client may only permit the use of Securnet HSCN within its organisation to a healthcare provider or an individual employed by or with a job role designed to provide services to the NHS.

It is the responsibility of Client to ensure that members of its own user community use Securnet services in an acceptable manner and in accordance with current legislation.

Disclaimer

IQVIA and PSL 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 is accepted for any inaccuracies.

Securnet - Acceptable Use Policy ("AUP")

Introduction

The purpose of this AUP is to enable IQVIA and PSL to protect the integrity of Securnet so that at all times it will be available to serve the needs of Client. To achieve this, IQVIA and PSL must be certain that Client will use Securnet responsibly and in accordance with this policy.

As Securnet is a closed network, 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 Securnet cannot protect their systems from the actions, legitimate or otherwise, of other local users. A thorough understanding of the Security Policy document and of professional guidance on protecting the privacy and security of clinical data is essential. You shall also meet the requirements of the UK Data Protection Act 2018 and the European Union General Data Protection Regulation (GDPR), the Privacy and Electronic Communications (EC) Regulations 2003 as amended and superseded in the UK from time to time ("Data Protection Legislation") at all times and you will fully comply with the Data Protection Legislation as it applies to the relevant part of the UK, at all times. You acknowledge and agree that you are the Controller in respect of the Personal Data that you process through the HSCN and NHS Digital, IQVIA and PSL have no liability or responsibility to Data Subjects in respect of the same, save that NHS Digital will act as a Processor in respect of such Personal Data in respect of which it has made the commitments below. You shall ensure you have a legal basis for processing the Personal Data and have informed all Data Subjects of the purpose of processing their Personal Data and that their Personal Data will be transferred to and processed by third parties through your use of the HSCN . You shall be fully responsible and liable to NHS Digital, IQVIA and PSL for any failure by you or your representatives to process the Personal Data in accordance with this AUP or otherwise in accordance with the Data Protection Legislation and shall accordingly indemnify in full IQVIA, NHS Digital and PSL for any loss, liability, fine, claim, damages, costs and expenses suffered or incurred arising out of your failure to comply with the data protection obligations in this document or under the Data Protection Legislation. "Processor", "Controller", "Data Subject" and "Personal Data", "Special Categories of Data" and "process" shall have the meaning set out in the Data Protection Legislation. Notwithstanding the foregoing, NHS Digital shall process the following Personal Data as a Controller and Client hereby agrees to such processing: (a) traffic data (including IP addresses) used to transmit data over HSCN; (b) customer relationship management data required to resolve queries about HSCN; (c) other data required for the administration of HSCN. Client shall be solely responsible for all Personal Data placed on the HSCN and shall implement appropriate organizational and technical measures to ensure the security of the Personal Data commensurate with the level of risk posed by the processing

NHS Digital Processor Commitments

NHS Digital has committed to:

1. *process the Personal Data only on documented instructions from the Client, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;*

2. *ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;*

3. *take all measures required pursuant to Article 32 of GDPR;*

4. *respect the conditions referred to in paragraphs 2 and 4 of Article 28 of GDPR for engaging another processor;*

5. *taking into account the nature of the processing, assist the Client by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Client's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of GDPR;*

6. *assist the Client in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to NHS Digital;*

7. *at the choice of the Client, delete or return all the personal data to the Client after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the personal data;*

8. *make available to the Client all information necessary to demonstrate compliance with the obligations laid down in these paragraphs 1 to 8 and allow for and contribute to audits, including inspections, conducted by the Client or another auditor mandated by the Client.*

Client acknowledges and agrees IQVIA and PSL shall have no liability for any failure by NHS Digital to comply with the data processing clauses above and that all claims for any such failures shall be made by the Client directly to NHS Digital.

The NHS requires all HSCN users to comply with all applicable information governance requirements in order to handle patient data and access systems, services and resources that are available through the HSCN in relation to the use of NHS Digital National Applications. In particular, all user organisations with access to HSCN shall complete the Data Security and Protection Toolkit, (including all assertions and mandatory evidence items) or any replacement for the Data Security and Protection Toolkit as may be issued by the NHS.

Please read this AUP document carefully and ask the Securnet Service Centre if you have any questions.

Acceptable Use

Client may use Securnet for the purpose of interworking with other User Organisations, and with organisations attached to networks that are reachable via interworking agreements operated by Securnet.

Subject to the following bullet points, use of Securnet is restricted to normal business activity that is in furtherance of the aims and policies of Client.

The HSCN must solely be used for legitimate purposes associated with the sharing of information within the health and social care community.

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

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

Unacceptable Use

Securnet may NOT be used for any of the following:

(a) 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;
(b) the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety;

(c) the creation or transmission of defamatory material;
(d) the transmission of material such that this infringes the copyright of another person;
(e) the transmission of unsolicited commercial or advertising material either to other User Organisations, or to organisations connected to other networks;
(f) non-healthcare profit making activity that grossly abuses the service;
(g) 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;
(h) gross abuse of the service by the unsolicited sending of inappropriate e-mail to large numbers of people, whether on Securnet, or on the Internet.
(i) deliberate unauthorised access to facilities or services accessible via Securnet;
(j) deliberate activities with any of the following characteristics:
    a. flagrant wasting of staff effort or networked resources, including the effort of staff involved in the support of those systems;
    b. corrupting or destroying other users' data;
    c. violating the privacy of other users;
    d. disrupting the work of other users;
    e. using Securnet in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
    f. continuing to use an item of networking software or hardware after IQVIA has requested that use cease because it is causing disruption to the correct functioning of Securnet;
    g. other misuse of Securnet or networked resources, such as the introduction of "viruses".

Where Securnet is being used to access another network such as HSCN any abuse of the acceptable use policy of that network will be regarded as unacceptable use of Securnet.

Note that this list is not exhaustive, and can be updated in IQVIA's sole discretion (acting reasonably).

If you are in doubt about whether you may use Securnet for a particular purpose, you should seek advice from the Securnet Service Centre.

It is not permitted to provide access to Securnet by third parties without the prior agreement of IQVIA and Client must have in place technical and organizational measures to prevent third parties from routing traffic through the HSCN. Nothing in this document authorizes you to re-sell your connection to the HSCN,

Compliance

It is the responsibility of Client to take all reasonable steps to ensure compliance with the conditions set out in this AUP and to ensure that unacceptable use of Securnet does not occur. The discharge of this responsibility must include informing those within the relevant organisation with access to Securnet of their obligations in this respect.

All changes to the connected environment must be communicated to the Securnet Service Centre.

If IQVIA, NHS Digital or PSL has reasonable grounds to believe that Client's use of resources and the HSCN may contravene the requirements of this AUP then IQVIA, NHS Digital and PSL reserve the right to restrict or to terminate the connection, during which time Client's obligation to pay the Service Fees will continue. If access has only been restricted and not terminated then once the issue has been remedied to the satisfaction of the Securnet security teams, the connection will be restored.

If NHS Digital has reasonable grounds to believe that Client's use of resources may contravene any NHS policy (including without limitation if the NHS has concerns over cyber security, information assurance or information governance requirements, that the Client is undermining the availability of HSCN, damaging the reputation of HSCN, the NHS or Her Majesty's Government or otherwise poses a security threat) then IQVIA and PSL reserves the right to restrict or to terminate the connection, during which time Client's obligation to pay the Service Fees will continue. If access has only been restricted and not terminated then once the issue has been remedied to the satisfaction of NHS Digital and the Securnet security teams, the connection will be restored.

Where violation of these conditions is illegal or unlawful, or results in loss or damage to IQVIA and/or Securnet resources or the resources of third parties accessible via Securnet, the matter may be referred for legal action.

If you are given notice of any investigation into a security matter or penalty relating to a contravention of this AUP, you may appeal to IQVIA via the Securnet Service Centre within 14 days of such notice being given.

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

If you should become aware that your staff or colleagues are breaching this AUP then you must report this to the Securnet Service Centre immediately.

Security Policy

Data held by Client needs to be protected from any unauthorised access. This should be undertaken in the following ways;

i) Client's system must have adequate staff identification and authentication controls.

ii) Client 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. iii) The HSCN does not ~~help~~ secure data in any way as it passes across the network.

Personally identifiable clinical data that is transmitted over Securnet must be protected by cryptographic services conforming to current NHS standards at all times.

You should be aware that the NHS mandates network monitoring on the HSCN, which includes the monitoring of the connection point between all providers such as Securnet and the HSCN as well as the monitoring and inspection of unencrypted internet-bound traffic.

You must protect the security and privacy of other User Organisations using Securnet by the following means:

(a) Your organisation must have a virus protection policy in place.
(b) All data/files which Client sends or receives over Securnet, 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 at least every week by mechanisms appropriate to your software.
(c) Client must have clear, documented policies preventing staff from using Securnet for illegitimate purposes, data that has been accessed via Securnet 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.
(d) Where the Securnet connection for the HSCN is direct into individual sites it must only be established from a workstation on the local LAN segment.
(e) For national applications the application will be deemed as acceptable to provide adequate security into and out of Securnet and the HSCN providing the client applies management controls in their own local area network environment to ensure the risk to Securnet and the HSCN is minimised.

1. The workstation/LAN segment should be located in a secure environment where appropriate physical access control can be exercised.
2. All incidents that constitute a threat to Securnet or HSCN security must be reported to the Securnet Service Desk immediately and reasonable co-operation provided to resolve the incident.
3. You must ensure that physical access to the Securnet router and ancillary equipment is restricted to only authorised personnel.

Client agrees to work with NHS Digital, IQVIA and PSL in relation to any security concern they may have including without limitation helping to contain the problem, minimize the impact, subsequently resolve it and help prevent a reoccurrence.

In the event of a security incident that relates to your use of the HSCN you agree to:

1. conduct initial diagnosis of the incident to determine which service is the cause or likely cause;

2. raise the issue with IQVIA and PSL;

3. at the earliest opportunity notify NHS Digital through the notification mechanism within the HSCN website and complete actions assigned by NHS Digital, IQVIA or PSL or their respective representatives within the timescales required by the same;

4. deal with contacts from the HSCN Data Security Centre to resolve incidents as if they were your client or users;

5. provide audit logs holding user activities, exceptions and information security events to assist investigations.

You must have robust data handling and security policies which cover the following:

1. a duty to be good citizens to help ensure HSCN is available for all users;

2. a duty to protect your and other users' information, systems and services from unauthorised disclosure, theft, unavailability or loss of integrity through cyber and other forms of attack.

You acknowledge and agree:

1. that the HSCN Authority Network Analytic Service will monitor the connection point between your networks and the HSCN for the purposes of maintaining the availability of the HSCN, systems and / or services that are available through the HSCN, and the connection between the HSCN and the internet. Examples include looking for abnormal amounts of traffic that could indicate a malware or other cyber security attack. However, the HSCN Authority Network Analytic Service does not look at or store the content of network traffic.

2. that the HSCN Authority's Advanced Network Monitoring Service will monitor and inspect, through signature and behavioural analysis, the content of unencrypted internet-bound traffic to look for evidence of malicious or suspicious content.

3. that the operation of this service involves the analysis of the content of internet traffic, including Personal Data and Special Categories of Personal Data (as each term is defined in in the Data Protection Legislation.

4. NHS Digital, IQVIA and PSL shall have no liability to you in respect of the functioning or non-functioning of the HSCN Authority Network Analytic Service and/or the HSCN Authority's Advanced Network Monitoring Service.

5. the HSCN's primary requirement is to be available as a means for sharing information between the health and social care community;

6. the HSCN does not help secure data in any way as it passes across the network. Responsibility for providing sufficient security lies with the sending and receiving organisation, or the providers and users of sites or applications that are accessed through the HSCN. This includes providing assurances that any service or application available on the HSCN or any organisations or users on the network are authentic and appropriately secured; and

7. NHS Digital, IQVIA and PSL do not warrant the authenticity of any service, system or data available through the HSCN or of any information received through the HSCN;

8. Because there is sometimes a business need to access a variety of content from a range of services, the HSCN network does not impose any restrictions on categories of sites or services that HSCN Consumers can access through the HSCN, except that: for internet access, a standard set of controls are in place to prevent data from being shared with known malware resources (for example, places on the internet with which malware may try to communicate with). The purpose of this restriction is to limit the impact on the HSCN community should a malware attack take place, and as such the list of blocked sites may change from time to time; and you may agree access restrictions on internet access or general network access

(for example, blocks on categories of internet sites) with IQVIA and PSL, but that is a solely a matter between the you and IQVIA and PSL;

9. to provide and maintain (through their connection profile information posted at the HSCN Website – Providers of NHS Services section): whether their connection to the HSCN is shared with any other organisations (whether health and social care or not) and if so the identity of those organisations; and the following contacts at the Client: the business sponsor of the connection – this contact should be in a senior position in the organisation who is ultimately responsible for the use of the HSCN Connectivity Services (e.g. Chief Information Officer); and security lead with whom NHS Digital, IQVIA and PSL can communicate security information. This individual may be the Senior Information Risk Officer (SIRO), Caldicott Guardian, Chief Security Officer or of equivalent standing and responsibility. For some Clients, this may be a contact at for example, a partner organisation such as an IT systems supplier or shared service provider who handles security matters for the Client.

You shall comply with all applicable information governance requirements in order to handle patient data, and access systems, services and resources that are available through the HSCN. For the NHS Digital National Applications, this is currently the Data Security & Protection Toolkit (DSPT). For other systems and services, local arrangements may apply

The current arrangements for the NHS Digital National Applications are set out at the following location:

https://www.dsptoolkit.nhs.uk

You should check with organisations that provide systems and services that they use as to local arrangements that are in place.

You shall comply with all relevant policies, guidelines or directions from time to time made available on the HSCN Data Security Centre websites and other sources, accessible at the following locations (and/or via any replacement sites identified by NHS Digotal, IQVIA and PSL from time to time):

https://digital.nhs.uk/services/data-and-cyber-security-protecting-information-and-data-in-health-and-care; and

http://systems.digital.nhs.uk/infogov; and

https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles; and

https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/nhs-and-social-care-data-off-shoring-and-the-use-of-public-cloud-services; and

https://www.nist.gov.