Information Governance Statement of Compliance v6.0

1 Purpose

1.1 Context

1.1.1 The Information Governance Statement of Compliance (IGSoC) is the agreement between NHS Connecting for Health (NHS CFH) and Approved Service Recipients (ASRs) that sets out the terms and conditions for use of NHS CFH services.

1.1.2 The IGSoC contains a number of obligations regarding the use of NHS CFH services, and should be reviewed carefully before signing.

1.1.3 Organisations with existing access to NHS CFH services are required to complete an IGSoC and comply with its terms and conditions.

1.1.4 Advice is available for organisations to help meet the terms and conditions of the IGSoC. Applications for assistance and enquiries should be directed to the IGSoC Team at IGSoC@nhs.net. Further information is available at http://www.connectingforhealth.nhs.uk/igsoc.

1.2 Scope

1.2.1 The IGSoC is the agreement between NHS CFH and any organisations with access, directly or indirectly, to NHS CFH services including the NHS Care Records Service (NHS CRS) and includes obligations to maintain the confidentiality, integrity, security, availability and accuracy of personal data used in these services.

1.2.2 Indirect access is when NHS CFH services are received via an ASR and are not specifically authorised by NHS CFH, i.e. use of N3.

1.2.3 It is essential that every ASR meets its obligations in the IGSoC to the required standards in order to preserve the confidentiality, integrity, availability and accuracy of NHS information. By requiring that ASRs achieve the information governance standards incorporated in the terms and conditions of the IGSoC, NHS CFH can help to ensure appropriate safeguards are in place to protect NHS CFH services for all users.

1.2.4 The IGSoC is applicable to all organisations that use NHS CFH services, either directly or indirectly.

1.2.5 The terms and conditions in the IGSoC apply to other services operated and managed locally that might impact on NHS CFH services if IGSoC conditions are not applied, i.e. the use of virus checking software.

1.2.6 Variations to these terms and conditions are not permitted without the prior written agreement of NHS CFH.

1.2.7 This IGSoC replaces all previous agreements and versions.

1.2.8 The IGSoC should also be read in conjunction with a number of supporting documents, policies and guidance available from the NHS CFH website at http://www.connectingforhealth.nhs.uk/igsoc, http://www.igt.connectingforhealth.nhs.uk and http://nww.connectingforhealth.nhs.uk/ist (requires N3 access or email igsoc@nhs.net for details).

1.2.9 Printed copies of this document should be treated as out of date. The most up to date version is available from the NHS CFH website www.connectingforhealth.nhs.uk/igsoc.

2 Policy

2.1 No organisation is allowed to receive or connect to any NHS CFH services, including N3, unless they first comply with the terms and conditions of the IGSoC or by separate arrangement with NHS CFH (in the case of organisations such as other Government departments) and have submitted and had approval of their IGSoC declaration from NHS CFH.

2.2 Completion of the Information Governance Toolkit to the required standard and submission of the RA01 (where applicable) are prerequisites of IGSoC submission. An IGSoC approved by NHS CFH is required before access to services is granted.

2.3 This policy is applicable to every individual legal organisation connecting to or using any NHS CFH service, including N3.

2.4 Intermediary organisations providing services to other organisations, that are dependent on services from NHS CFH, are also required to complete the IGSoC and to ensure that all organisations that receive services are covered under separate valid IGSoCs.

2.5 Intermediary organisations are required to provide NHS CFH details of any organisation that has access, directly or indirectly, to NHS CFH services.

2.6 ASRs are required to maintain a local log, available for inspection on demand, of organisations to which they have allowed access through their firewall. This log is to be reviewed at least quarterly and unnecessary access rights removed.

3 Legislation

3.1 ASRs must have policies, standards, procedures and systems in place to ensure that they comply with all relevant UK and European legislation and be able to provide evidence, where appropriate, on demand.

3.2 British and European Standards/Industry Best Practice

3.2.1 ASRs should have achieved, or be working towards achieving; ISO27001 or other appropriate and relevant standards and best practice and are able to provide evidence, where appropriate, on demand.

3.3 NHS Policy

3.3.1 ASRs are expected to implement DH and NHS policies and good practice guides, where relevant, and be able to provide evidence of having done so on demand. See clause 1.2.8 for details.

3.4 NHS Connecting for Health Policy

3.4.1 ASRs will meet NHS CFH standards at all times and comply with all relevant policies. ASRs must be able to provide evidence, where appropriate, on demand. See clause 1.2.8 for details.

4 Terms and Conditions

4.1 IGSoC General

4.1.1 Use of services or facilities provided by the NHS CFH is for ASRs and their Authorised Users only, and in accordance with the requirements for those services.

4.1.2 NHS CFH services are provided to organisations to enhance patient care. NHS CFH services are not intended, unless expressly stated otherwise, for use by patients.

4.1.3 Each completed and accepted IGSoC can cover only one individual legal organisation, unless one organisation is hosted by another and has its information governance policies and procedures set and monitored by the host and the host agrees that it is responsible for the hosted organisation’s compliance and monitors it for such. Reference should be made to clause 4.1.10 to ensure compliance.

4.1.4 The IGSoC applies to every service or facility delivered, or to be delivered, by NHS CFH, and its contracted Service Providers, or by NHS CFH compliant system suppliers to an ASR and for use by its Authorised Users.

4.1.5 NHS CFH reviews system accesses and data processing involving any services provided by NHS CFH and its Service Providers, to ensure their acceptable usage and reliability in accordance with the terms and conditions of the IGSoC and Information Governance Toolkit.

4.1.6 Organisations are not authorised to access NHS CFH services unless an IGSoC submission has been completed, submitted and approved by the NHS CFH IGSoC Team.

4.1.7 By signing and submitting the IGSoC, the Authorised Signatory agrees to accept future versions of the IGSoC in order to continue receiving NHS CFH services.

4.1.8 The ASR will be notified of changes to the IGSoC in advance of new versions becoming effective, using the email address provided on the initial IGSoC form or later notified in writing.

4.1.9 This agreement may be terminated by either party at any time. The organisation may then have its services from NHS CFH ceased.

4.1.10 The ASR is required to enforce, through local disciplinary or contractual measures, where necessary, the Information Governance standards and processes including, where appropriate, the registration process and adherence to conditions identified in the RA01 registration form signed by its Authorised Users.

4.1.11 If there are any changes to the ASR's legal status, i.e. change to its name, merger with another organisation or anything that otherwise changes its legal status, the new organisation must resubmit an IGSoC.

4.1.12 In the event that NHS CFH changes the conditions of being an ASR, it may require the organisation to reaffirm their compliance or otherwise with the relevant changes at that time.

4.1.13 Contents of this IGSoC must not be altered or modified from their original state.

4.1.14 Use of the Airwave service shall be in accordance with the Airwave Codes of Connection and Practice (as amended from time to time) and made available to Airwave users.

4.1.15 The services provided by NHS CFH to the ASR must be used for accessing NHS CFH accredited systems and services and not for inappropriate browsing of other internal and internet systems.

4.1.15.1 Inappropriate browsing of the Internet shall be defined by the ASR, through an Acceptable Usage Policy (AUP) made available to all local Authorised Users. Such policies shall indicate the scope and extent to which users may make use of these network services, including specific guidance on access to the Internet.

4.1.15.2 Inappropriate browsing of internal systems shall be defined as anyone attempting unauthorised access to any system connected to the N3 environment without permission from that system owner.

5 Information Governance

5.1 The ASR should appoint a person to have responsibility for the security management of the ASR's network connection(s) and their locally connected systems.

5.2 ASR shall manage their networks and connected systems in accordance with their local policies written to incorporate the requirements of IGSoC clauses 3.2, 3.3 and 3.4.

5.3 NHS CFH services should be protected against unauthorised viewing. Inactivity timeout settings, set in accordance with NHS CFH policy, should be embodied in the organisation's security policy, enforced and monitored through local policies and procedures.

5.4 Access to NHS CFH infrastructure and connected systems are subject to appropriate access and authentication controls that meet the NHS CFH Information Governance standards (as amended from time to time). Those services not applicable to Smartcard access and authentication control should have suitable policies, procedures, processes, controls and monitoring to ensure NHS CFH standards are met.

5.5 The use of NHS CFH provided infrastructure or services for unauthorised advertising or other non-healthcare related activity is expressly forbidden and must not be undertaken.

5.6 NHS organisations may make limited use of NHS CFH provided infrastructure to access services via the Internet as might normally be required to carry out business activities that contribute to the care of patients, subject to the level of use not being detrimental to the quality of service received by other users of NHS CFH services and of a nature not likely to bring the NHS into disrepute.

5.7 NHS organisations with a substantial requirement for non-NHS commercial activities must make separate arrangements and not use the NHS CFH provided standard service or services for such purposes.

6 Services covered

6.1 Any and all types of communications, including wireless communications, used by the ASR associated with services delivered by NHS CFH and its contracted Service Providers or by NHS CFH compliant system suppliers.

7 Information Governance Toolkit

7.1 An Information Governance framework, appropriate to the organisation type, is delivered and periodically updated in the NHS Information Governance Toolkit and Registration Authority guidance.

7.2 ASR must meet NHS CFH information governance requirements as identified in the NHS Information Governance Toolkit. Compliance with the IGSoC is reconfirmed annually through submission of the IGT to the appropriate level.

8 Incident Reporting

8.1 In the event of an identified or reported service problem or incident, relevant support staff may be required to investigate and resolve those problems by accessing the functions and data affected. All such problem management activity shall be subject to NHS CFH information governance controls.

8.2 The ASR shall have a process for internal information security audit and management of alerts. This process should be tested for compliance at least twice in any twelve-month period.

8.3 Unauthorised access must be considered for appropriate action by the system owner. ASRs are strongly advised to provide network management facilities, e.g. caching and filtering, that permit the permission or prohibition, and logging of internet usage for the purposes of providing appropriate reporting to line management and forensic reporting as defined in their Acceptable Use Policy (AUP). Disciplinary action necessary in response to reported abuse should be detailed in the AUP, staff contracts or other local policies.

8.4 The ASR acknowledge that, if required to process personal data (as the term ‘personal data’ is defined in section 1(1) of the Data Protection Act 1998), in the course of providing the NHS CFH services, it shall do so only on the instruction of an appropriate Data Controller and shall maintain in place, having regard to the state of technological development and the cost of implementation, all appropriate measures, procedures and policies to protect the security and integrity of any such personal data.

8.5 Any threat or security event affecting or potentially affecting the security of NHS CFH provided infrastructure or services must be immediately reported via the NHS CFH incident reporting arrangements and/or other contacts provided by NHS CFH, for example the local RA manager for Smartcard incidents.

9 Audit

9.1 IGSoC compliance checks are required annually. Compliance monitoring is through annual NHS CFH Information Governance Toolkit returns for ASRs or other forms of assurance required by NHS CFH.

9.2 The ASR shall allow NHS CFH, or its representatives, to carry out ad-hoc on-site audits as necessary to confirm compliance with these terms and conditions.

10 Logical Connection Architecture

10.1 Any connections to other systems or networks that are not covered by an approved IGSoC must either be disconnected or comply with a security mechanism specifically approved by the NHS CFH IGSoC team. If an ASR is in doubt over its compliance, the NHS CFH IGSoC team must be consulted for advice and guidance.

10.2 ASRs shall ensure that all users (both Authorised Users and other personnel accessing IT) in their organisation, who may impact the performance/security of NHS CRS and/or services, are aware they must not connect or reconfigure computer/network devices or load software which has not been notified where necessary to or authorised in advance by the ASR according to the highest standards and good practice guidance published by NHS CFH (as occasionally amended) Department of Health or provided by the NHS Connecting for Health IGSoC team.

11 Sponsorship (third party organisations only)

11.1 Non-NHS organisations are required to provide written evidence, in a standard form, that their requirement to receive services is supported by an NHS organisation.

11.2 In the event that sponsorship for a service expires, access to this service will be withdrawn.

11.3 In the event that all sponsorship expires and is not replaced, NHS CFH retains the right to deactivate service access.

12 Offshore Requirements

12.1 ASRs shall ensure that they meet the requirements of DH and NHS CFH policy on personal data leaving England, or being viewed from overseas, by completing and complying with the Information Governance Offshore Support Requirements.

12.2 A copy of the Information Governance Offshore Support Requirements is available on request or can be downloaded from http://www.connectingforhealth.nhs.uk/igsoc.

13 IGSoC Approvals Process

13.1 The IGSoC must be completed by the Authorised Signatory and returned to NHS CFH using the process specified below.

13.2 The IGSoC is a part of the process for approving requests for connections and services from NHS CFH, directly or indirectly, and must be completed before a connection or service will be activated. Refers to clause 2.1.

13.3 On successful completion of an IGSoC submission, the requesting organisation will become an Authorised Service Recipient of NHS CFH services.

13.4 The IGSoC (appendix A) together with any other required information or documentation, as stated on the IGSoC website, should be completed by the Authorised Signatory and submitted via email to IGSoC@nhs.net.

13.5 The submitting email must originate from the mailbox of the Authorised Signatory. A copy of the completed IGSoC submission should be retained for the ASR's Information Governance records.

13.6 The Authorised Signatory must notify NHS CFH the name, job title and contact details of nominated delegates with authority to raise change to service requests on behalf of the organisation. These should be listed in the IGSoC form below. Changes to these should come from the Authorised Signatory by email to IGSoC@nhs.net.

13.7 Compliance is further assured by a combination of additional audits by the Healthcare Commission, Authorised Service Recipients and ad-hoc audits by NHS CFH or its authorised representatives.

13.8 NHS CFH reserves the right to communicate via any means the status of IGSoC and supporting submissions to appropriate interested parties.

Appendix A – Information Governance Statement of Compliance

<Insert date here>

To the NHS Connecting for Heath IGSoC Team;

I confirm, on behalf of *<Insert Organisation name here>*, that I have read, understood and agree to comply with the terms and conditions of the Information Governance Statement of Compliance and acknowledge that failure to maintain compliance may result in the withdrawal of NHS Connecting for Health services.

My organisation is an *<Insert IGT view name here>*. I have provided the supporting documentation required and will notify NHS CFH of any changes to the content of these. NB Requirements are listed on the Information Governance Statement of Compliance website.

Our connection is provided by *<insert company name here>*, their contact email address and phone number are *<insert contact details here>*.

The NACS code for my organisation is *<insert NACS Code here>*.

The named contacts listed below have the delegated authority to commit this organisation to changes, new orders and to allow third party access to systems and services:

Name	Job Title	Email	Telephone

Yours,
Signed:
Name:
Job Title:
Telephone:
Email:

Once completed in accordance with instructions, submit to **IGSoC@nhs.net**

The information you provide will be used by NHS Connecting for Health for purposes of the management and administration of the Information Governance Statement of Compliance. NHS Connecting for Health will pass the contact details you provide onto your Service Provider for the purposes of managing your organisations' connectivity securely. It will not be disclosed or used for any other purpose without your permission, which will be sought prior to any such use or disclosure. NHS Connecting for Health undertake to keep your information secure until the time when it is no longer required, at which time it will be destroyed by secure means (in accordance with the Data Protection Act 1998). You may be contacted by your Service Provider for maintenance and improvement purposes of your connection. If you require further information NHS Connecting for Health can be contacted at mailto:igsoc@nhs.net.

Address for correspondence: http://www.connectingforhealth.nhs.uk/contact

Glossary of terms

Acceptable Use Policy	A policy that sets out the use, frequency, appropriateness and volume of use that is and is not acceptable
Aggregator	An Aggregator is the provider of the N3 service necessary to access NHS CFH applications
Airwave	Airwave is the national digital radio communications network dedicated to the emergency services.
Approved Service Recipient (ASR)	The organisation whose IGSoC statement of compliance has been accepted by NHS Connecting for Health and has been approved to receive its services.
Authorised Signatory	The individual, with executive status and legal liability, able to commit their organisation to the obligations of the IGSoC and swiftly put in place any action plans necessary to correct deficiencies in compliance. This must be the most senior person in the organisation, typically Senior Partner, CEO, MD, Owner, Sole Proprietor, etc.
Authorised User	Any person authorised to use NHS Connecting for Health services or healthcare related applications or has been issued a Smartcard
DH	Department of Health
Digital Services	Digital Services are those networking, communications and applications services provided by the NHS Connecting for Health that comprise and are collectively known as the NHS National Programme for IT (NPfIT)
Incident Reporting	Incident Reporting concerns the formal identification and reporting of perceived or actual events with the potential to cause the physical or logical loss of or damage to the IT assets of the NHS CFH and its services providers, or causing failure, disruption or discredit to its services
Information Governance	Information Governance is the structures, policies and practice of the DH, the NHS and its suppliers to ensure the confidentiality and security of all records, and especially patient records and to enable the ethical use of them for the benefit of individual patients and the public good.
Information Governance Toolkit (IGT)	The Information Governance Toolkit is the on-line self-assessment tool that contains the expected IG standards, best practice methods and guidelines applicable to NHS information services generally.
N3	The National Network for the NHS, the NHS's own network
NACS	The National Administrative Code Service. It is responsible for the national policy and standards with regard to organisation and practitioner codes. These code standards form part of the NHS data standards.
NHS CFH	NHS CFH means NHS Connecting for Health.
NHS CRS	NHS Care Record Service (an NHS Connecting for Health service)
NPfIT	National Programme for Information Technology
Organisation	The legal entity that supports or utilises NPfIT services, (i.e. GP practice, Partnership, Limited Company, Public Limited Company and other legal organisations).
Policy/ Policies	All references to policy and policies includes, but is not limited to, guidance, good practice guides, guidelines, standards, procedures and other materials, however titled, found at NHS CFH website at http://www.connectingforhealth.nhs.uk/igsoc, http://www.igt.connectingforhealth.nhs.uk and http://nww.connectingforhealth.nhs.uk/ist (requires N3 access or email igsoc@nhs.net for details)
Registered Users	Registered Users these are all personnel employed or contracted in the organisation who have been approved to receive services
Smartcards	Smartcards are plastic cards containing an electronic chip (like a chip and PIN credit card) that is used to access the NHS Care Records Service and other National Programme for IT applications, along with a Passcode.