

	<b>NHS Confidential</b>			
	<b>Offshore Support Requirements</b>			
	Programme	<i>NPFIT</i>	<b>DOCUMENT RECORD ID KEY</b>	
	Sub-Prog / Project	<i>Digital Information Policy</i>	<i>NPFIT-FNT-TO-IG-IGCOM-0102.01</i>	
	Prog. Director	<i>Mike Walker</i>		
	Owner	<i>Phil Walker</i>	Version	<i>2.0</i>
	Author	<i>Phil Walker</i>		
Version Date	<i>30 April 2009</i>	Status	<i>Final</i>	

## Information Governance Offshore Support Requirements

### Amendment History:

Version	Date	Amendment History
1.1	22 April 2009	Update of version 1.0
1.2	23 April 2009	Update to version 1.1 by A Donaldson
1.3	27 April 2009	Update to v1.3 by P Walker to reflect comments by Raj Samani
2.0	30 April 2009	No further amendments

### Reviewers:

This document must be reviewed by the following. Indicate any delegation for sign off.

Name	Signature	Title / Responsibility	Date	Version
Raj Samani		Chief Security Officer	24/4/09	1.2

### Approvals:

This document requires the following approvals:

Name	Signature	Title / Responsibility	Date	Version
Martin Bellamy		Director of Programme & System Delivery	30/4/09	1.3

# Information Governance

## 1. Overview

This document provides the Information Governance requirements for cases where remote support and maintenance services are provided by Support Service Providers from a location outside of the borders of England for the support of system and application software and hardware components. Whilst it is intended primarily for those systems and applications that are connected to the N3 Network or to other NHS CFH systems and applications, it also provides Good Practice Guidelines to be followed for all similar arrangements.

The key principle is that risk should be assessed and managed using an Information Security Management System (ISMS) throughout the support lifecycle, e.g. from initial system planning and development through to system decommissioning. To support the ISMS an information risk assessment should be carried out by the Authority, Support Service Provider and Data Controller organisation that considers the impacts in terms of confidentiality, integrity and availability. Such potential impacts may go beyond the boundary of the asset under review and where this is the case others should be alerted to any risks likely to affect their assets. The risk assessment should be carried out in accordance with Department of Health guidance on managing information risk using appropriate and approved risk assessment methodologies or frameworks<sup>1</sup>. Sensitivity should be shown when dealing with the outcome of the risk assessment and should be protectively marked and handled using strict security mechanisms.

An Information Security Management System (ISMS, as detailed in ISO27001 Information Security standard) should be documented by the Support Service Provider that is related to the risk assessment and approved by the Authority. Periodically the Authority will review the Security Management Plan with the Support Service Provider and request evidence to demonstrate compliance.

At the highest level, new applications for N3 connectivity in respect of support services are managed through the following sequence:

- i. Sponsorship letter from the relevant data controller and confirmation of requirement by the Authority N3 team.
- ii. Assurance statement and IGT assessment completed by the support Service Provider (an data controller if not already in place). Process supported by DH Information Policy.
- iii. Logical technical security architecture design and Penetration Testing approved by the Authority Infrastructure Security team.
- iv. Approval by the authority.

---

<sup>1</sup> DH guidance is provided via the NHS Information Governance Toolkit located at: <https://www.igt.connectingforhealth.nhs.uk/>

## 2. Definitions

- "processing", in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including-
  - (a) organisation, adaptation or alteration of the information or data,
  - (b) retrieval, viewing, consultation or other use of the data,
  - (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
  - (d) alignment, combination, blocking, erasure or destruction of the information or data
- "data controller" means a person/body that (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;
- "data processor", in relation to personal data, means any person/body (other than an employee of the data controller) who processes the data on behalf of the data controller;
- the use of the term "data" shall mean any Personal Data and/or Sensitive Personal Data in addition to any other data within the Service;
- "patient identifiable data" is personal information that can be used to establish the identity of an NHS patient.
- references to an "organisation" shall be references to an entity constituted by statute;
- Support Service Provider shall refer any organisation providing the offshore support and maintenance service;
- Service shall be use to mean the entire support and maintenance contracted elements, including helpdesk services, remote resolution, subsequent levels of support, remote patching and fixes, support staff, infrastructure, etc;
- the use of the term "user" or "User" shall mean any user of the Service including, without limitation, members of the Support Service Provider's support staff.

### 3. Requirements

Sanctions may potentially apply to the Support Service Provider where significant information or infrastructural risks are identified, or where information incidents have arisen that suggest a significant IG shortfall exists.

Requirements	
<b>1</b>	In respect of systems and applications connected to NHS CFH systems and applications Patient Identifiable Data should not be recorded outside of the England boundary in any format for any reason without the prior explicit written permission of NHS CFH.
<b>2</b>	Where it is proposed that there be a significant change to where data is to be processed which patients are unaware of and may have concerns about, the Data Controller shall consider and document its policy in respect of: <ol style="list-style-type: none"> <li>i. obtaining consent from the patients whose information will be held on the system; and</li> <li>ii. satisfying fair processing requirements with respect to the Data Protection Act 1998.</li> </ol>
<b>3</b>	A logical technical security architecture design should be documented by the Data Controller and the Support Service Provider and approved by the Authority. Any subsequent changes to this architecture must be flagged to the Authority for reconsideration.
<b>4</b>	The Support Service Provider must complete an assessment of performance utilising the NHS Information Governance Toolkit and provide an assurance statement indicating that all key requirements are satisfied and agreement that this may be audited by the Authority.
<b>5</b>	Appropriate training and communications should be provided by the Support Service Provider to ensure that all support staff having any contact with the remote support and maintenance service are informed of the requirement not to record any Patient Identifiable Data.
<b>6</b>	The Support Service Provider shall develop a process for the destruction of Patient Identifiable Data which it receives or inadvertently records through communications or other means with the users. This process should be compliant with the "Records Management: NHS Code of Practice" guidance published in April 2006, or as subsequently updated.
<b>7</b>	The Support Service Provider should periodically, minimum annually, scan all information repositories and stores within the Support Service Provider's base location(s), outside of England, for the presence of Patient Identifiable Data, and if any found securely deleted immediately.
<b>8</b>	The Support Service Provider shall ensure all support staff working within the Service have had reliability and security clearance checks carried out that include <ul style="list-style-type: none"> <li>• Identity (passport, etc.);</li> <li>• Employment, academic and qualification references including any relevant previous security checks which should be followed up in writing.</li> </ul>
<b>9</b>	The Support Service Provider shall ensure that any visitors, or contractors, that require access to the Service, are vetted to the same level as support staff, sign the confidentiality statement and have all access recorded for audit purposes.

<b>10</b>	The Support Service Provider shall ensure all support staff working within the Service, who may have access to patient identifiable data, sign a confidentiality agreement with the Support Service Provider.
<b>11</b>	The Support Service Provider shall be required to implement and maintain an Information Security Management System (see ISO27001 "Information Security standard"). Evidence of current attainment should be available on request.
<b>12</b>	The Support Service Provider shall be required to undertake a security penetration test before the approval to proceed to live production use is granted. This penetration test should be planned, witnessed and reviewed in conjunction with the Authority and where necessary an agreed corrective action plan documented.
<b>13</b>	All access to Patient Identifiable Data should be recorded in a tamperproof audit log and stored on-site in England, including viewing, creation, amendments and deletions. The information recorded should enable the Data Controller to inform patients who has accessed their information, when, what they saw and what action was taken.
<b>14</b>	The Support Service Provider should provide physical security measures to ensure the connection, including communications equipment, to the Data Controller is protected against unauthorised access or unapproved use.
<b>15</b>	The Support Service Provider shall ensure that all communication links to the offshore location from the Data Controller that are used for accessing patient identifiable data are protected through the appropriate use of approved end-to-end encryption. This should also apply to all re-routed links where planned for resilience purposes.
<b>16</b>	The Support Service Provider should maintain an information asset register of all equipment, including desktops, used in providing the remote support and maintenance service and a copy of must be passed to the Authority. Any material changes affecting the information asset register should be approved by the Authority, prior to the changes being implemented, and the information asset register must be provided to the Authority for inspection on request.
<b>17</b>	The Support Service Provider shall ensure that access to laptops and peripheral storage devices, e.g. all removable media such as USB devices, used as part of the Service is only permitted to Authority approved individuals and that all such devices are encrypted to the Department of Health required standard.