Data Encryption Policy

*Please be aware that this printed version of the Policy may NOT be the latest version. Staff are reminded that they should always refer to the Intranet for the latest version.*

<table>
<thead>
<tr>
<th>Purpose of Agreement</th>
<th>This document describes the NHS Solent Policy on data encryption and employees’ responsibilities for ensuring that personal identifiable/business critical information is stored and transferred securely.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Type</td>
<td>Policy ☒, SOP ☐, Guideline ☐</td>
</tr>
<tr>
<td>Reference Number</td>
<td>IG15</td>
</tr>
<tr>
<td>Version</td>
<td>2</td>
</tr>
<tr>
<td>Name of Approving Committees/Groups</td>
<td>IGSsC, NHSLA Policy Information Asset Owner Forum, Information Asset Custodian Forum,</td>
</tr>
<tr>
<td>Operational Date</td>
<td>November 2013</td>
</tr>
<tr>
<td>Document Review Date</td>
<td>November 2016</td>
</tr>
<tr>
<td>Document Sponsor (Name &amp; Job Title)</td>
<td>Judy Hillier Director of Nursing &amp; Quality &amp; Caldicott Guardian</td>
</tr>
<tr>
<td>Document Manager (Name &amp; Job Title)</td>
<td>Shelley Brown Information Governance Lead</td>
</tr>
<tr>
<td>Document developed in consultation with</td>
<td>IGSsC, NHSLA Policy Information Asset Owner Forum, Information Asset Custodian Forum,</td>
</tr>
<tr>
<td>Intranet Location</td>
<td>N/A</td>
</tr>
<tr>
<td>Website Location</td>
<td>Policies/Operational Policies</td>
</tr>
<tr>
<td>Keywords (for website/intranet uploading)</td>
<td>Data encryption policy, information, data, encryption, policy, IGSG, governance, Personal Identifiable Data, PID, P.I.D., Mobile Data Devices, laptops, Blackberry’s, palm tops, pda, personal digital assistants, USB memory sticks, CD, DVD, data loss,</td>
</tr>
</tbody>
</table>
information governance toolkit, NHSmail, nhs.net, information governance steering group, corporate services team
Information Asset Owners, IAO’s, IAOS, monitoring, transfer of data, removable media
### Amendments Summary:

<table>
<thead>
<tr>
<th>Amend No</th>
<th>Issued</th>
<th>Page(s)</th>
<th>Subject</th>
<th>Action Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Feb 12</td>
<td></td>
<td>Logo &amp; Name Change</td>
<td>Feb 12</td>
</tr>
<tr>
<td>1</td>
<td>Feb 13</td>
<td></td>
<td>Review Date change</td>
<td>Feb 13</td>
</tr>
<tr>
<td>1</td>
<td>Aug 13</td>
<td></td>
<td>Sponsor change</td>
<td>Aug 13</td>
</tr>
<tr>
<td>1</td>
<td>Aug 13</td>
<td>5</td>
<td>Revision to scope details</td>
<td>August 13</td>
</tr>
</tbody>
</table>

### Review Log

Include details of when the document was last reviewed:

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Review Date</th>
<th>Name of Reviewer</th>
<th>Ratification Process</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>30.08.13</td>
<td>S. Brown</td>
<td>Policy Steering Group</td>
<td>This policy forms Part of the Management Framework Strategy in relation to Information Governance.</td>
</tr>
</tbody>
</table>
DATA ENCRYPTION POLICY

Table of Contents

1. INTRODUCTION & PURPOSE ................................................................. 5
   1.1. Introduction .................................................................................... 5
   1.2. Purpose ......................................................................................... 5

2. SCOPE & DEFINITIONS .................................................................... 5
   2.1. Scope .......................................................................................... 5
   2.2. Definitions ................................................................................... 5

3. PROCESS/REQUIREMENTS .............................................................. 6
   3.1. Rationale ...................................................................................... 6
   3.2. Requirements .............................................................................. 6
   3.3. Areas of Risk .............................................................................. 6
   3.4. Encryption Strategy .................................................................... 7

4. ROLES & RESPONSIBILITIES ......................................................... 8
   4.1. IT Department ............................................................................. 8
   4.2. Information Governance Team .................................................... 9
   4.3. Departmental Managers/Information Asset Owners (IAO's) ....... 9
   4.4. Users ......................................................................................... 9

5. TRAINING ...................................................................................... 10
   5.1. Training Implications ................................................................ 10

6. EQUALITY & DIVERSITY AND MENTAL CAPACITY ACT ......... 10
   6.1. Equality Statement ..................................................................... 10
   6.2. Discrimination ........................................................................... 10

7. SUCCESS CRITERIA / MONITORING THE EFFECTIVENESS OF THE
   POLICY ................................................................................................ 10
   7.1. Audit .......................................................................................... 10
   7.2. Auditing & Monitoring Criteria ................................................... 10
   7.3. The Care Quality Commission Standards ................................... 11
   7.4. Policy Breaches ......................................................................... 11

8. REVIEW .......................................................................................... 11

9. REFERENCES AND LINKS TO OTHER DOCUMENTS .............. 11
   9.1. Links to Other Policies ................................................................. 11

Appendix 1: Encrypted Memory/USB sticks- Form EMSApp1 .......... 13
Appendix 2: Transfer of Data on Removable Media ....................... 14
Appendix 3: Impact Assessment ......................................................... 16

R:\IG Solent\Policies & Agreements\Policies\Data Encryption\
20131212_DataEncryptionPolicy_V2.doc
1. INTRODUCTION & PURPOSE

1.1. Introduction
It is paramount that Solent NHS Trust has the ability to protect all personal
identifiable/business critical information from unauthorised access,
disclosure or loss.
The Trust will use an appropriate software encryption package.

1.2. Purpose
This document sets out the Trust’s policy for the use of Encryption for
organisational purposes.

2. SCOPE & DEFINITIONS

2.1. Scope
This policy applies to all directly and indirectly employed staff and other
persons working within the Trust in line with Solent NHS Trust Equality
Statement.
This policy forms Part of the Management Framework Strategy in relation
to Information Governance.

This policy covers all electronically stored data, held on both static and
mobile devices.

This policy is complementary to other Trust Policies and should be used /
read in conjunction with them.

2.2. Definitions
- Personal Identifiable Data (PID) – means data which relates to an
individual who can be identified from that data as defined in the Data
Protection Act 1998.

- Encryption – a process of scrambling data unless authorisation is given to
the user to view it.

- Mobile Data Devices – this includes any mobile device that can store data.
This will include laptops, Blackberry’s, palm tops (or personal digital
assistants), USB memory sticks, CD/DVD etc.

- Business Critical Information – where the loss of data would have a
significant impact on the performance, reputation and operational
effectiveness of the organisation. This may include but is not limited to
Financial, personal, major projects.
• Virtual Private Network (VPN) – allows a user with appropriate authority to connect to the Trusts network from a remote location via the internet.

3. PROCESS/REQUIREMENTS

3.1. Rationale
The need for encryption has increased due to the loss of data from several public sector organisations as reported in the media. Solent NHS Trust recognises the need to secure its data, protect its staff and patients and have strict control over data in transit. This has also become a mandatory requirement, in accordance with Gateway Reference 10509 (September 2008).

The deployment of the encryption solutions will prevent unauthorised access to patient identifiable and/or business critical information, based on a risk assessed criteria.

3.2. Requirements
• National NHS procurement of software
• Requirements under the Information Governance Toolkit
• ISO 27001: Information Security Management Standard
• Gateway reference 10509 (letter to Chief Executives dated September 2008)

3.3. Areas of Risk
The listing below identifies the risks the Trust may be subjected to:

Emailing personal identifiable/business critical information - NHSmail has been mandated as the only permitted method of emailing personal identifiable data (PID), both the sender and receiver must have NHSmail accounts or similar Government approved encrypted mail systems.

Laptops – are the most common form of mobile device holding mobile data. This form of mobile computing is increasing within the Trust, and there is a high risk that they can be lost or stolen. A laptop that does not have any form of encryption can allow unauthorised access to the data contained on it, and, so, must be protected. The IT Department will install and manage the encryption software across all Trust laptops.

USB memory sticks and USB connected hard drives or similar – these drives have the potential to store large quantities of data and therefore will
need to be fully encrypted using hardware / device encryption and a justified case made for their use.

Desktop PCs – should be risk assessed and those identified at risk must be encrypted with full disk encryption.

Port lockdown is proposed to be installed as part of the new Solent IT provider contract.

Note: it is Trust policy that data should not be stored on the local hard drive so it would only be desktops which have a valid business reason to store data locally and are in vulnerable locations that would require encrypting.

Other mobile devices – including Blackberry’s, PDA’s, smart phones, CD, iPhones, iPad or DVD’s. The loss of any of these devices containing sensitive data would compromise the Trust’s information security if there was not robust encryption in place. Again, it is the user’s responsibility to make sure that these devices are encrypted and used within the scope of this policy.

3.4. Encryption Strategy
To comply with national mandatory requirements the Trust has adopted the following strategies:

NHSmail - was agreed as the only permitted method of emailing Personal Identifiable Data (PID), both the sender and receiver must have NHSmail accounts or similar Government approved encrypted mail systems. Staff are able to register for an NHS Mail account at the NHS.net website, http://www.nhs.net

All Trust owned mobile computing devices used for the storage or transfer of personal identifiable/business critical information must be fully encrypted.

All Trust laptops must be encrypted. Auto-boot was decided as the method of encryption as it enabled the Trust laptops to be encrypted as quickly as possible. Laptops are automatically encrypted when connected to the local NHS network.

USB memory sticks - the Information Governance Steering Sub Committee (IGSsC) decided that for the transfer of personal identifiable/business critical information the organisation would issue encrypted memory sticks once a risk assessment is approved by a Manager and signed off by an IG team member and where no alternative
secure means of accessing or transporting the data can be found. (See Appendix 1 Encrypted Memory/USB sticks- Form EMSApp1)

Permit non-encrypted memory sticks for non-PID storage (such as presentations).

Departments using such devices will remain responsible for the safekeeping and recovery in the event of staff leaving the organisation as with any other piece of Trust equipment

Desktop PCs – should be risk assessed and those identified at risk must be encrypted with full disk encryption.

Other mobile devices – including Blackberry’s, PDA’s or smart phones must be encrypted to the national standard. The loss of any of these devices containing sensitive data would compromise the Trust’s information security if there was not robust encryption in place.

CD & DVD’s – only if there is an approved business reason to put PID onto CD or DVD, then the media must be encrypted as per the ICT procedure. (See Appendix 2).

Users’ privately owned mobile computing equipment or related devices (e.g. laptops, PDAs, mobile phones) will not be permitted to connect to the Trust network nor to access Trust network resources. The only exception to this rule will be via VPN remote access which is tightly controlled technically and monitored through policy.

Other removable devices may be added on an ongoing basis if it is deemed that there is a potential need for data to be downloaded to these. However, these will be fully encrypted in line with this policy. All authorisations for reading and writing to any other mobile devices must be granted by the user’s manager by the completion of an authorisation form (see Appendix 2). In cases involving high volumes of data, a Risk Assessment may be required.

All mobile devices classified within the scope of this policy must be encrypted to the national standard to prevent the possible loss of any Trust data.

Only Trust owned authorised mobile devices may be used.

4. ROLES & RESPONSIBILITIES

4.1. IT Department
The IT Department will be responsible for:-
• The implementation of encryption on all Trust Laptop’s and approved mobile data devices, including the facility for content encryption and the training in its use;

• The support and maintenance of this system via the IT helpdesk function;

• Managing changes to the configuration of the service.

4.2. **Information Governance Team**

Within the Trust, the Information Governance Team will be specifically responsible for:

• Approving the business case and issuing encrypted memory sticks;

• Approving the business need for writable access to be given to staff for the use of CD/DVD/other writable devices;

• The purchasing of devices to the required standard;

• Monitoring of this policy.

4.3. **Departmental Managers/Information Asset Owners (IAO’s)**

Managers are responsible for:-

• Approving the business case for the issue of USB encrypted memory sticks for their departmental staff using the form at Appendix 1;

• Approval of the procedure at Appendix 2 for the encryption of PID on CD/DVD/other writable devices and forwarding these to the Corporate Services Team for approval, who will forward to the ICT Services Security Specialist for management.

4.4. **Users**

Each individual member of staff and all other users given approved access to Trust information are responsible for guarding against the loss or disclosure of any PID/business critical information;

• Users must keep their username and password confidential in line with Trust policies. As with conventional passwords, encryption passwords should not be written down or shared.
• Users must download information from mobile devices to the secure network as soon as possible and once stored successfully then deleted from the mobile device.

5. TRAINING

5.1. Training Implications
There are no specific training implications associated with the implementation of this policy.

6. EQUALITY & DIVERSITY AND MENTAL CAPACITY ACT

6.1. Equality Impact Assessment
This document has been subject to an Equality Impact Assessment in accordance with the Trust’s Race Equality Scheme and Disability Equality Scheme, see Appendix 3 Impact Assessment.

6.2. Discrimination
This policy is considered to be compatible with the Human Rights Act and does not discriminate against any group.

7. SUCCESS CRITERIA / MONITORING THE EFFECTIVENESS OF THE POLICY

7.1. Audit
The Trust reserves the right to monitor the activity of individuals in relation to the use of PID/business critical information on all Trust equipment both static and mobile. The ICT Services Security Specialist will carry out audits on a regular basis to ensure compliance with this policy.

All actual or suspected IG incidents must be reported to the appropriate Risk Management Team; identify and address the causes, manage the risks highlighted and share the lessons learnt across the organisations.

7.2. Auditing & Monitoring Criteria

<table>
<thead>
<tr>
<th>Monitoring requirements</th>
<th>a) Ensure encryption is installed on all mobile devices and media</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>b) Ensure that no patient identifiable/business critical information is sent out of the Trust without encryption</td>
</tr>
<tr>
<td></td>
<td>c) Monitor compliance with the policy</td>
</tr>
</tbody>
</table>


The Care Quality Commission Standards
The Care Quality Commission have replaced Standards for Better Health for monitoring a series of key standards issued by the Department of Health, which serve as indicators of the quality of care to be delivered across the NHS in England. Below are the definitions of the Domains within these standards.

<table>
<thead>
<tr>
<th>Domain</th>
<th>Definition/Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety</td>
<td>To minimise the risk of patient identifiable data/business critical information being available to unauthorised parties.</td>
</tr>
<tr>
<td>Governance</td>
<td>To enable the Trust to safeguard its patient identifiable data/business critical information in line with national standards.</td>
</tr>
</tbody>
</table>

7.3. **Policy Breaches**
Any breach of this policy may result in the Trust’s disciplinary policy being invoked.

8. **REVIEW**
This document may be reviewed at any time at the request of either at staff side or management, but will automatically be reviewed two years from initial approval and thereafter on a biennial basis unless organisational changes, legislation, guidance or non-compliance prompt an earlier review.

9. **REFERENCES AND LINKS TO OTHER DOCUMENTS**

9.1. **Links to Other Policies**
- Information Security Policy
- Registration Authority Policy
- Registration Authority Procedure Manual
- Network Security Policy
- Web Services Policy
• Antivirus Policy
• Information Governance Strategy
• Information Governance Policy
• Data Protection Act, Caldicott & Confidentiality Policy & Procedures
• Storage of Electronic Information on Network Drives Procedure
• Access to Personal & Health Records Procedure
• Disciplinary Policy
• Please complete a risk assessment to justify the use of an encrypted USB
  
  20120315_IGRiskAssessment_Template_V2

• Appendix 1: Encrypted Memory/USB sticks- Form EMSApp1

All trust staff will be responsible for the acceptable use of the Trust’s information, information systems and data networks. Heads of service and Data custodians will be responsible for the physical security of IT assets located within their respective departments.

All Trust staff will be compliant with the information security policy. Failure to do so could result in disciplinary action.

Name of staff member requesting encrypted memory stick:
(please print full name)

Role/designation of staff member:

Signature:

Contact details
Phone:
Email:

Has a risk assessment been completed fully and attached:
Y/N

Date:

When completed please send to one of the SNHS.SolentIGTeam@nhs.net for approval:
Manager to complete box below:

<table>
<thead>
<tr>
<th>Name: (please print)</th>
<th>Signature:</th>
<th>Role/Designation:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Date: Email:
Risk assessment attached: Y/N Phone:
## Removable media

- Procedure for copying data on removable media

### Document Information

<table>
<thead>
<tr>
<th>Prepared by</th>
<th>David Tyrie</th>
<th>PC Support Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document classification</td>
<td>Commercial in confidence</td>
<td></td>
</tr>
<tr>
<td>Version number</td>
<td>0.2</td>
<td>0.2</td>
</tr>
<tr>
<td>Issued</td>
<td>6th December 2007</td>
<td>7th December 2008</td>
</tr>
<tr>
<td>Review Date</td>
<td></td>
<td>procedure</td>
</tr>
<tr>
<td>Document status</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Document History

<table>
<thead>
<tr>
<th>Version No.</th>
<th>Date</th>
<th>Change</th>
<th>By</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>06/12/2007</td>
<td>Draft</td>
<td>David Tyrie</td>
</tr>
<tr>
<td>0.2</td>
<td>10/12/2007</td>
<td>Incorporate changes suggested by Andrew Hale</td>
<td>David Tyrie</td>
</tr>
</tbody>
</table>

### Related documents

Reference: Relates to Connecting for Health Guidance issued August 2006 by Information Security to ICT Services. Reviewed and reissued by email to all ICT IT staff as dated above.

Title
Connecting for health GPG
Transfer of Data on Removable Media

Context

Situations may arise which require Personal Identifiable Data to be transferred within the NHS, or shared with authorised third parties, on removable media such as writable CD/DVD, memory sticks, or through the use of internet services such as email. The following provides guidance on the proper handling of this data to ensure confidentiality.

Guidance

The minimum encryption standard for transferring sensitive data across the N3 (N3 is the national broadband network for the English National Health Service (NHS), connecting all NHS locations and 1.3 million employees across England) Wide Area Network is 112 bit Triple DES is the common name for the Triple Data Encryption Algorithm. This standard is available when using applications such as Pretty Good Privacy (PGP) which is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting and decrypting texts, e-mails, files, directories and whole disk partitions to increase the security of e-mail communication or WinZIP (used to compress large files) version 9 or later. With these products the data can be put into a Self Decrypting Archive (SDA), as the software that created the archive does not need to be installed on the recipient’s computer.

The passphrase for the archive must be of an appropriate length and complexity, that is to say, a minimum of 25 characters which comprise alphanumeric, upper case characters, and punctuation.

The information must of course be encrypted and be in the form of:

- A ‘Self Decrypting Archive’ (SDA) attached to an email, providing the passphrase is forwarded to the recipient by alternate means separately from the SDA, such that the SDA and passphrase cannot be associated.
- An SDA on CD, DVD or other removable media containing the data is delivered to or collected by a representative from the organisations involved. An email (or other communication entirely separate from the SDA) providing the passphrase is sent to the recipient.

If the SDA is sent by non-electronic means, check that the removable media has been safely received by the recipient.
### Appendix 3: Equality Statement

#### Step 1 – Scoping: identify the policies aims

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. What are the main aims and objectives of the document?</td>
<td>To outline the process for Data Encryption and standard operating procedures within Solent NHS Trust</td>
</tr>
<tr>
<td>2. Who will be affected by it?</td>
<td>All staff and any contractors or commercial Third party contractors processing data on behalf of Solent NHS Trust</td>
</tr>
<tr>
<td>3. What are the existing performance indicators/measures for this? What are the outcomes you want to achieve?</td>
<td>Information Governance Toolkit annually measures our compliance with Data encryption standards.</td>
</tr>
<tr>
<td>4. What information do you already have on the equality impact of this document?</td>
<td>None</td>
</tr>
<tr>
<td>5. Are there demographic changes or trends locally to be considered?</td>
<td>Solent NHS Is formed by the merger of both Southampton City &amp; Portsmouth city provider services. AS both cities are ‘Ports’ there is a transient demographic population.</td>
</tr>
<tr>
<td>6. What other information do you need?</td>
<td>N/A</td>
</tr>
</tbody>
</table>

#### Step 2 - Assessing the Impact; consider the data and research

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
<th>Answer (Evidence)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Could the document unlawfully against any group?</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Can any group benefit or be excluded?</td>
<td>x</td>
<td></td>
<td>Applies to all staff groups</td>
</tr>
<tr>
<td>3. Can any group be denied fair &amp; equal access to or treatment as a result of this document?</td>
<td>X</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>4. Can this actively promote good relations with and between different groups?</td>
<td>X</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>5. Have you carried out any consultation internally/externally with relevant individual groups?</td>
<td>X</td>
<td></td>
<td>Current NHSLA Policy Group members consulted and wider groups represented by PSG members. Information Governance Group members.</td>
</tr>
<tr>
<td>6. Have you used a variety of different methods of consultation/involvement</td>
<td>X</td>
<td></td>
<td>Via email and face to face meetings</td>
</tr>
<tr>
<td>Mental Capacity Act implications</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Will this document require a decision to be made by or about a service user? (Refer to the Mental Capacity Act document for further information)</td>
<td>X</td>
<td></td>
<td>Does not apply to patients</td>
</tr>
</tbody>
</table>

If there is no negative impact – end the Impact Assessment here.

#### Step 3 - Recommendations and Action Plans

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Is the impact low, medium or high?</td>
<td></td>
</tr>
<tr>
<td>2. What action/modification needs to be taken to minimise or eliminate the negative impact?</td>
<td></td>
</tr>
<tr>
<td>3. Are there likely to be different outcomes with any modifications? Explain these?</td>
<td></td>
</tr>
</tbody>
</table>

#### Step 4- Implementation, Monitoring and Review

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. What are the implementation and monitoring arrangements, including timescales?</td>
<td>Already implemented, monitored annually.</td>
</tr>
</tbody>
</table>
2. Who within the Department/Team will be responsible for monitoring and regular review of the document? | The Head of Information Governance

<table>
<thead>
<tr>
<th><strong>Step 5 - Publishing the Results</strong></th>
<th><strong>Answer</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>How will the results of this assessment be published and where? (It is essential that there is documented evidence of why decisions were made).</td>
<td>The Information Governance Toolkit annual assessment</td>
</tr>
</tbody>
</table>