# Data handling and storage policy

## Issue sheet

<table>
<thead>
<tr>
<th>Document reference</th>
<th>NHSBSARM017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document location</td>
<td>S:\BSA\IGM\Managing IG\Developing Policy and Strategy\Develop or Review DHS Policy\Current and Final</td>
</tr>
<tr>
<td>Title</td>
<td>NHSBSA Data handling and storage policy</td>
</tr>
<tr>
<td>Author</td>
<td>Rachel Hardiman</td>
</tr>
<tr>
<td>Issued to</td>
<td>All NHSBSA staff</td>
</tr>
<tr>
<td>Reason issued</td>
<td>For information / action</td>
</tr>
<tr>
<td>Last reviewed</td>
<td>10 March 2016</td>
</tr>
</tbody>
</table>

## Revision details

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Amended by</th>
<th>Approved by</th>
<th>Details of amendments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1</td>
<td>15.11.2010</td>
<td></td>
<td>IGSG</td>
<td></td>
</tr>
<tr>
<td>Version 2</td>
<td>31.03.2015</td>
<td>C Gooday</td>
<td>RMF</td>
<td>Updated name of CFSMS and applied new Government Information Classification scheme</td>
</tr>
<tr>
<td>Version 3</td>
<td>21.03.2016</td>
<td>C Gooday</td>
<td>RMF</td>
<td>Updated to reflect clear explanation of Official sensitive and remove public category</td>
</tr>
</tbody>
</table>
1. Introduction

1.1. The information held by the NHS Business Services Authority (NHSBSA) represents one of its most valuable assets. It is therefore essential that all information for which it has responsibility is used, communicated, transferred, stored, and disposed of in a manner that complies with legal and regulatory requirements, and with the broader information management and security framework of the NHSBSA.

1.2. Appropriate handling and storage of information is the responsibility of every member of staff in the NHSBSA. The technical processes in use to facilitate this are ineffective unless the correct procedures are carried out in a careful and consistent manner.

1.3. The NHSBSA is committed to properly protecting the information that it holds. This policy and associated practices and procedures have been agreed by the NHSBSA Leadership Team and Senior Management of the Authority.

2. Policy statement

2.1. Exceptions: NHS Protect maintain their own policies relating to data handling and storage and are therefore not included in the scope of this policy.

2.2. This document defines the Data Handling and Storage (DHS) Policy for the NHSBSA.

2.3. The DHS Policy applies to all information obtained and processed by the NHSBSA and the NHSBSA’s employees, and by contractors and other third-party service providers in their relations with the Authority.

2.4. This document:
   - Sets out the NHSBSA’s policy for the use, communication, transfer, storage, and disposal of all information obtained and processed
   - Establishes the responsibilities for DHS

3. Scope of this policy

3.1. The DHS Policy supplements the NHSBSA’s primary policies relating to information governance, security and management. The DHS should be read in conjunction with these policies:
   - NHSBSAIGM002 Information Governance Policy
   - NHSBSAIS001 Information Security Policy
   - NHSBSARARM001 Records Management Policy
3.2. The policy should also be read in conjunction with other policies, tools and procedures, most notably:
   - NHSBSAIS004 Mobile Computing Policy
   - NHSBSA Data Classification Matrix
   - NHSBSAIS002 Information Security Incident Reporting Procedure
   - NHSBSADPN001 Data Protection Policy
   - NHSBSARM015 Corporate Records Management Guidance

3.3. The policy is concerned with all information systems, digital and non-digital, and will cover all information within the NHSBSA that is or may be:
   - stored on computers
   - transmitted across networks
   - printed out or written on paper
   - sent internally or externally by post, courier, or fax
   - stored on removable and other electronic media
   - Spoken in face-to-face conversation or over the telephone.

3.4. The policy will apply to all divisions, sites and departments in the NHSBSA, to all NHSBSA staff and as appropriate to its contractors and third-party service providers.

3.5. The policy establishes the security classification of information used by the NHSBSA and the different handling and storage requirements in respect of each.

4. Security classification of information

4.1. Information created and received by the NHSBSA should be classified according to sensitivity of its contents. Classification and controls should take account of organisational needs for sharing or restricting information, and the associated impacts and risks, e.g. unauthorised access or damage to the information.

4.2. The classification used within the NHSBSA for all information is OFFICIAL.
   Information classified as OFFICIAL includes:

   Non-sensitive information, such as:
   - Brochures
   - News releases
   - Marketing materials
   - Routine correspondence where there is no confidentiality requirement.
   There may be a requirement to protect the integrity and the Availability of this type of information.

   Transactional information, such as:
   - One-off exchanges with third parties including members of the public which may include personal, commercial or financial information.
There is a requirement to protect the Confidentiality, Integrity and Availability of this type of information to avoid disruption to service delivery, commercial or financial impact.

Routine NHSBSA business, such as:
- Employee newsletters
- Internal phone directories
- Inter-office memoranda
- Non person-identifiable information
- Internal policies and procedures
- Routine correspondence with third parties and members of the public which may contain some personal or commercial information

There is a requirement to protect the Confidentiality, Integrity and Availability of this type of information.

Legally Defined information, such as
- Personally Identifiable information as defined by the Data Protection Act.
- Financial information

There is a clear requirement to protect the Confidentiality, Integrity and Availability of this type of information.

Consequences if OFFICIAL information is mishandled:
- Unauthorised disclosure would not significantly impact NHSBSA, or any of its stakeholders, including members of the public, or employees

Protective Marking
- There is no requirement to explicitly mark routine OFFICIAL information.

4.3. There is a subset of information handled by the NHSBSA where the inappropriate use of the information could have damaging consequences for the NHSBSA, for an individual (or group of individuals), or other organisations. This information, which is caveated OFFICIAL-SENSITIVE, includes:
- Patient and customer information
- Details of staff appointments before they are announced
- Staff personnel file and Electronic Staff Records
- Pay and expenses of staff below Band 8B
- Information that could be used to compromise the security of NHSBSA information such as internal IP addresses, details of security measures and versions of security products.
- Commercial or market sensitive information such as details of potential supplier bids prior to contract award, pricing schedules, customer details, details of unique aspects of a business model, tender information for unsuccessful bidders;
- Information about investigations and civil or criminal proceedings that could compromise public protection or enforcement activities, or prejudice court cases;
- Legal opinions provided by legal professions
• Information about where controlled drugs can be dispensed or which could lead to this being deduced;
• MP Correspondence, especially during an election;
• Risk Registers;
• papers for a future board meeting;
• the most sensitive NHSBSA corporate or operational information, e.g. relating to organisational change planning, contentious negotiations, or major security or business continuity issues;
• policy development and contentious and very sensitive issues;

Consequences if information is mishandled:
• Unauthorised disclosure likely to result in significant adverse impact, embarrassment or penalties to NHSBSA, its stakeholders, employees, or members of the public.

Protective Marking
• Where there is a clear and justifiable requirement to reinforce the “need to know”, information should be conspicuously marked: "OFFICIAL–SENSITIVE"

The OFFICIAL-SENSITIVE caveat should not be confused with a separate classification; it is tool to denote OFFICIAL information that is of a particular sensitivity. Further details of the Government Security Classification definitions are available in Annex B.

5. Information access

5.1. Internal and external access to information held by the NHSBSA, and to the systems within which it is held, is governed by the security classification of the information.
• OFFICIAL information is either generally available to the public or all staff on a need-to-know basis, as decided by their line manager
• Official Sensitive information is available only to staff who have a business need to know the information, and with the written approval of the Information Asset owner

5.2. Where access to Official Sensitive information has been authorised, use of such data shall be limited to the purpose required to perform NHSBSA business.

5.3. Where a member of staff who has access to Official Sensitive information either leaves or has their authorisation removed e.g. as a result of secondment or change or role, their status must be updated within 24 hours by, e.g., changing access control lists.
6. Transfer and exchange of information

6.1. Information and data can be transferred and exchanged in a variety of ways, both direct and indirect. These include:
- Spoken word
- Post, fax, or e-mail
- Internet or intranet
- Magnetic media (including CDs, DVDs, Memory Sticks and Data Cartridges)
- Electronic File Transfer
- Web Portals (i.e. NHSBSA web-enabled applications)
- Print, Film, Fiche, Video, DVD Images

6.2. Information must only be transferred to persons who are authorised to have access to it. There must be adequate security measures in place at the virtual and/or physical destination. Where Official Sensitive information is being transferred, Information Asset Owners will typically require additional assurance around the security measures in place.

6.3. Official Sensitive information should not be sent or physically taken off-site without the appropriate authorisation by the Information Asset Owner or their delegated authority and security measures (e.g. encryption).

6.4. The proper use of the various means of transferring information is set out in the NHSBSA Data Classification Matrix. This must be adhered to at all times.

6.5. The transfer and exchange of information concerning identifiable living persons is additionally subject to NHSBSADPN001 Data Protection Policy.

7. Storage and protection of information

7.1. Information should be stored throughout its existence in an environment suited to its format and security classification, to ensure its preservation from physical harm or degradation and its security from loss or unauthorised access.

7.2. Information, whether original or duplicate, should never be kept outside corporate systems (e.g. on PC hard drives, on CDs or other removable media) except as a temporary off-line copy driven by a business need to work off-site or off-line, or for authorised transfer to other users or systems.

7.3. Information in all formats should be stored in conditions that protect it from threats to its physical integrity through unnecessary wear and tear; specific threats such as fire, flooding, and magnetic fields; and environmental extremes or fluctuations. Where appropriate, special storage equipment and environments should be used.
7.4. Information should be stored in systems and according to classifications, frameworks and procedures that enable it to be readily identified and retrieved throughout its existence.

7.5. Information held in digital formats should be managed and stored in such a way as to ensure usability and accessibility through time. This may involve migration of information between environments and systems, conversion to current software versions, or conversion from obsolete to current formats.

7.6. Physical access to information should be restricted by locking it in rooms, cabinets, drawers, and other storage areas or units, and by ensuring that files and computer monitors are not left open to general or casual view.

7.7. Protection from unauthorised access may require mechanisms such as password-protection or encryption of digital files and data, and sign-in sheets or request dockets for access to non-digital information.

7.8. Where information is stored on a mobile device (e.g. PDA, USB drive, laptop), special care must be taken to ensure that the device is physically protected from theft, loss, or damage, particularly if it is transferred or used away from NHSBSA sites.

7.9. The NHSBSA’s procedures and guidance on appropriate storage and protection of digital and non-digital information are set out in the following documents:
   - NHSBSA Data Classification Matrix
   - NHSBSARM015 Corporate Records Management Guidance
   - NHSBSAIS004 Mobile Computing Policy
   - NHSBSAIS001 Information Security Policy

8. Retention and disposal of information

8.1. The retention periods for all of the categories of information held by the NHSBSA are set out in NHSBSARM012 Corporate Records Retention Schedule. This applies to information in all formats and systems, and to both original and duplicate information.

8.2. Information may be subject to several disposal actions throughout its existence: typical disposal actions are
   - transfer to another department
   - transfer to a non-local storage facility (e.g. records centre, warehouse, off-line digital storage system)
   - transfer for permanent historical retention in a records office or archives
   - destruction
8.3. Information should only be destroyed in the ordinary course of business; no information subject to open or pending investigation, audit, or litigation should be destroyed.

8.4. Physical destruction of digital and non-digital media should be carried out to standards appropriate to the security classification of the information. Official Sensitive information must be destroyed securely, and the act of destruction should be certified or signed off.

8.5. Where electronic data is to be erased but the medium left intact, it must be deleted to the extent appropriate to the security classification, e.g. by over-writing files or reformatting disks.

8.6. The destruction processes appropriate to each security classification, for information held in digital or non-digital formats, are set out in the NHSBSA Data Classification Matrix.

9. Data handling and storage responsibilities

9.1. It is the role of the NHSBSA Leadership Team to define the NHSBSA’s policy in respect of DHS, taking into account legal and NHS requirements. The NHSBSA Leadership Team is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

9.2. The NHSBSA Leadership Team members, whilst retaining their legal responsibilities, have delegated DHS compliance to the NHSBSA Information Governance and Security Group (IGSG) and the Head of Internal Governance (HoIG).

9.3. The HoIG is responsible for overseeing day-to-day DHS issues; developing and maintaining – directly or by delegation – policies, standards, procedures and guidance; co-ordinating DHS in the NHSBSA; and raising awareness of DHS.

9.4. Managers within the NHSBSA are responsible for ensuring that this policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance.

9.5. All staff, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day-to-day basis.
10. **Validity of this policy**

10.1. This policy is designed to avoid discrimination and be in accordance with the HRA and its underlying principles.

10.2. This policy should be reviewed annually under the authority of the NHSBSA Leadership Team members. Associated DHS standards should be subject to an ongoing development and review programme.
Appendix A: References

Adams State College *Data Handling and Storage Policy* 1 Aug 2007
http://www.adams.edu/administration/computing/datahandling.pdf

Great Yarmouth Borough Council *Data Handling & Security Breaches* 17 Mar 2009

Highways Agency *Data Handling Policy* n.d.

University for the Creative Arts *Information Handling Policy* 20 Jul 2009

University of Leicester *Information Handling Policy* 16 Aug 2010
http://www2.le.ac.uk/offices/itservices/resources/cis/iso/pol/pdfs/s7.pdf

University System of Georgia *Draft USG Data Handling and Storage Policy* n.d.
Appendix B: Government Security Classifications

New Government Security Classifications (published April 2014) have been implemented to assist you in deciding how to share and protect information. Three simplified levels of security classifications for information assets are now in effect. The new levels are:

OFFICIAL
ALL routine public sector business, operations and services should be treated as OFFICIAL. NHSBBSA will operate exclusively at this level; including the subset categories of OFFICIAL-SENSITIVE: where applicable. See Table 1 for examples.

SECRET
Very sensitive government (or partners) information that requires protection against the highly capable threats, such as well-resourced and determined threat actors and highly serious organised crime groups.

TOP SECRET
Exceptionally sensitive Government (or partners) information assets that directly support (or threaten) the national security of the UK or allies and requires extremely high assurance or protection against highly bespoke and targeted attacks.