NHS
Business Services Authority

Data Classification, Handling and Storage Policy

Issue sheet

Document reference	ISMSPOL 082
Document location	- Security and Information Governance webpage on MYHUB - ISMS sub-folder under Control A.5
Title	Data Classification, Handling and Storage Policy
Author	Information Security Assurance Manager
Owner	Head of Security & Information Governance
Issued to	All staff
Reason issued	For action
Last reviewed	December 2020
Review Cycle	Annual
Date of Equality Assessment	No impact
Date of Fraud Review	No impact

Revision details

Version	Date	Amended by	Approved by	Details of amendments
1.0	15/11/2010		IGSG	
2.0	31/03/2015	C Gooday	RMF	Updated name of CFSMS and applied new Government Information Classification scheme
3.0	21/03/2016	C Gooday	RMF	Updated to reflect clear explanation of Official sensitive and remove public category
4.0	13/12/2018	Andrew Scullion	BISG (13 Nov 2018)	Streamline and re-baseline of Policy
5.0	18/11/2019	Andrew Scullion	To be discussed at BISG during Feb 2020	Annual Review
5.1	18/11/2020	Peter McCann		Transfer to new policy template and annual review Due for BISG approval – Nov 2020
5.2	09/12/2020	Peter McCann		Minor amendments in line with BISG feedback
6.0	09/12/2020	Peter McCann	BISG	Approved at BISG

1. Policy Statement and Authorities

1.1. This policy defines the NHS Business Services Authority's approach to data classification, handling and storage requirements. This policy gets its authority and approval from **ISMSPOL 001 Information Security Policy** and specifically the following objective/statement of intent;

The NHSBSA shall ensure that information receives an appropriate level of protection in accordance with its importance

1.2. The purpose of this Data Classification, Handling and Storage Policy is to ensure that the applicable and relevant security controls are set in place in line with ISO 27001 – Information Security Management System (ISMS) requirements, the Department for Health & Social Care, the wider NHS, the Security Policy Framework (SPF) and other HMG requirements.

1.3. This policy relates to all information systems, digital and non-digital, and covers all data 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 paper or electronic means
- stored on removable and other electronic media
- spoken in face-to-face conversation or over the telephone

2. Audience

2.1 This policy is intended to be read and understood by all NHSBSA staff, contractors, agency staff, suppliers and wider stakeholders where appropriate.

3. Exceptions

3.1 In this document the term **MUST** in upper case is used to indicate an absolute requirement. It is mandatory that all users comply with the requirements detailed in this standard unless a formal exception is raised. Failure to do so may lead to disciplinary action in line with the HR Disciplinary Policy and other associated policies such as the Equality and Diversity Policy.

3.2 Any exceptions to this policy **MUST** be raised initially with the NHSBSA Security & Information Governance team via the Information Security Policy Exception Management Process (ISMSPOL 023) and the Information Asset Owner (IAO) must be informed. Depending on the severity of the risk assessment, this may be escalated for approval to the Senior Information Risk Owner (SIRO) for formal review and approval.

3.3 Non compliances which are not raised as formal exceptions **MUST** be raised as a security incident – see NHSBSA Security Incident Management Standard Procedure on MYHUB.

3.4 Exceptions to this policy **MUST** be maintained on an appropriate risk register i.e. a team/functional risk register and/or ISMS and Cyber risk registers for accountability, traceability and security governance reporting to senior management.

4. Policy Statements

4.1 When handling data, all users **MUST** do so in accordance with and be responsible for adherence to the NHSBSA Data Classification, Handling and Storage Policy. Periodic auditing of adherence to this policy is the responsibility of the Security and Information Governance team

4.2 Users **MUST** ensure that data is appropriately labelled in accordance with HM Government Security Classification Policy (GSCP) and any bespoke requirements as required by the wider NHS. Further details of the Government Security Classification Policy definitions are available in Annex B.

4.3 The classification used within the NHSBSA for all information is **OFFICIAL**. The **OFFICIAL-SENSITIVE** handling caveat should be used where appropriate to denote **OFFICIAL** information that is of a particular sensitivity.

4.4 An approved level of protection must be used in the transfer of data in relation to its classification and privacy requirements.

4.5 Users **MUST** ensure data is transferred only to those who need to know, and that data shall be kept to the minimum required.

4.6 Any mishandling of data in transfer or at rest **MUST** be reported as a security incident in line with the NHSBSA Information Security Incident Management Procedure.

4.7 The transfer and exchange of information concerning identifiable living persons **MUST** be subject to the Data Protection and Confidentiality Policy. A Data Sharing Agreement (DSA) **MUST** be produced, agreed and signed by all parties prior to any NHS data containing Personal Data or **OFFICIAL-SENSITIVE** data/information being passed or shared with any organisation or body external to NHSBSA. Users must have authority (in writing) from the Information Asset Owner (IAO) to undertake the transfer.

4.8 The proper use of the various means of handling data **MUST** be followed as set out in the NHSBSA Data Classification Matrix in Annex A.

4.9 Users **MUST** ensure data is retained for the periods set out in the NHSBSA Corporate Records Retention Schedule.

4.10 Users **MUST** ensure data is destroyed securely in accordance with its classification, in accordance with NHSBSA Security Standards.

4.11 Information held in paper form **MUST** be securely destroyed in accordance with the NHSBSA Records Management Policy

4.12 The Security and Information Governance team should be approached where there is difficulty identifying a suitable method of transfer.

5. Compliance

5.1 In applying this policy, the NHSBSA will have due regard for the need to eliminate unlawful discrimination, promote equality of opportunity, and provide for good relations between people of diverse groups, in particular on the grounds of the following characteristics protected by the Equality Act (2010); age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, and sexual orientation, in addition to offending background, trade union membership, or any other personal characteristic.

5.2 Compliance with this policy **MUST** be subject to internal and external audit to ensure its effectiveness. The following methods to verify this include but are not limited to;

- Periodic documentation reviews
- Business tool reports
- Reporting within the security governance structure
- Internal and external audits
- Feedback to the policy and standard owner

6. Further Information

6.1 If you require any further information and guidance on the content of this policy, please contact the Information Security Team for further information.

Appendix A: Data Classification Matrix

Data Source	Categories	OFFICIAL	OFFICIAL-SENSITIVE
Transmission by Spoken Word	Conversation / Meetings	Ensure that you are not overheard	Private setting / lowered voices. Avoid public areas, e.g. elevators, hallways, cafeterias etc.
	Landline Telephones		Avoid proximity to unauthorised listeners. Speakerphone in secure area
	Mobile telephones (including voice enabled blackberries)		Use of analogue telephones discouraged, digital telephones preferred
	Voicemail or answering machines		Only leave name and contact details
Transmission by Post	Internal Mail within NHSBSA	No special handling required	Sealed inter-office envelope marked with the **OFFICIAL-SENSITIVE**
	External Mail within UK	2nd class mail. No special handling required	NHSBSA approved Secure Courier required so that delivery is recorded and traceable. 2 envelopes required: ● Outer envelope/package should clearly show the return address on the back. ● Inner envelope should be sealed and marked with the **OFFICIAL-SENSITIVE**
	External Mail outside of the UK	Secure Courier required so that delivery is recorded and traceable. Envelope/package should clearly show the return address on the back.	NHSBSA approved Secure Courier required so that delivery is recorded and traceable. 2 envelopes required: ● Outer envelope/package should clearly show the return address on the back. ● Inner envelope should be sealed and marked with the **OFFICIAL-SENSITIVE**
Transmission by Email	E-mail to recipients within the NHSBSA	Subject **should** be marked **OFFICIAL.** Ensure that the email address/es are for the correct recipient/s before sending.	Users **should** only share Personal Data over email for those who have a formal need to know. Subject **must** be marked **OFFICIAL-SENSITIVE.** Ensure that the email address/es are for the correct recipient/s before sending.

Data Source	Categories	OFFICIAL	OFFICIAL-SENSITIVE
	E-mail to recipients outside the NHSBSA	Subject **should** be marked **OFFICIAL.** Ensure that the email address/es are for the correct recipient/s before sending.	Users **should** only share Personal Data over email if a Data Sharing Agreement is in place Use of e-mail containing OFFICIAL**-SENSITIVE** data **must** be encrypted using the standard [SECURE] capability within NHSBSA. If other encryption method is used, you **must** check with nhsbsa.informationsecurity@nhs.net for latest and acceptable encryption standards. Broadcast to distribution lists is prohibited Data exchanges (even one-off events) **must** be subject to ISMSPOL 086 Data Protection and Confidentiality Policy. A Data Sharing Agreement (DSA) **must** be produced, agreed and signed by all parties prior to any NHS data containing Personal Data or **OFFICIAL-SENSITIVE** data being passed or shared with any organisation or body external to NHSBSA.
Transmission by Fax	Fax machines are inherently insecure and pose many risks to the NHSBSA. Their use should be as a back-up communication method only.	Use of a Fax Coversheet marked **OFFICIAL** is required. Not to be located in an area accessible to the general public. Telephone before transmission to ensure that recipient is waiting by the fax machine for the transmission. Subsequent telephone call to confirm successful receipt of the transmission	Prohibited unless an exception has been agreed with nhsbsa.informationsecurity@nhs.net
NHSBSA Intranet	My Hub	Content **should** be authorised by the head of service prior to submission for publishing	Content **should** be authorised by the head of service prior to submission for publishing Prohibited for Personal Data
Internet	NHSBSA Internet Webpages	Content and arrangements **must** be assured by nhsbsa.informationsecurity@nhs.net and authorised by the head of service prior to submission for publishing	Prohibited unless an exception has been agreed with nhsbsa.informationsecurity@nhs.net
	Broadcasting/uploading data to externally managed websites or web portals		
	Use of Cloud Services (SaaS / IaaS / PaaS)		Content and arrangements **must** be assured by nhsbsa.informationsecurity@nhs.net
Removable memory / media	Memory Sticks / USB Drives	Any removable media used to store NHSBSA information assets **must** be authorised and encrypted. Contact Security and Information Governance team for support at nhsbsa.informationsecurity@nhs.net	Prohibited unless an exception has been agreed with nhsbsa.informationsecurity@nhs.net Where exception is approved any removable media used to store NHSBSA information assets **must** be encrypted. Contact Security and Information Governance team for support at nhsbsa.informationsecurity@nhs.net
	CDs & DVDs	Prohibited unless an exception has been agreed with nhsbsa.informationsecurity@nhs.net Where exception is approved, any removable media used to store NHSBSA information assets **must** be encrypted. Contact Security and Information Governance team for support at nhsbsa.informationsecurity@nhs.net	Prohibited unless an exception has been agreed with nhsbsa.informationsecurity@nhs.net Where exception is approved, any removable media used to store NHSBSA information assets **must** be encrypted. Contact Security and Information Governance team for support at nhsbsa.informationsecurity@nhs.net

Data Source	Categories	OFFICIAL	OFFICIAL-SENSITIVE
	Hard Drives	Any removable media used to store NHSBSA information assets **must** be authorised and encrypted. Contact Security and Information Assurance team for support at nhsbsa.informationsecurity@nhs.net Magnetic Tape Hard Drives are Prohibited	Prohibited unless an exception has been agreed with nhsbsa.informationsecurity@nhs.net Where exception is approved, any removable media used to store NHSBSA information assets **must** be encrypted. Contact Security and Information Governance team for support at nhsbsa.informationsecurity@nhs.net
Electronic File Transfers	Setting up either a one-off or continuous transfer mechanism either within or outside of NHSBSA e.g. FTP, IPSEC or other VPN tunnels (not email – see above)	All electronic file transfers **must** be assured via the Security and Information Governance team at nhsbsa.informationsecurity@nhs.net before the first transfer is undertaken. The channel **should** be encrypted.	All electronic file transfers **must** be assured via the Security and Information Governance team at nhsbsa.informationsecurity@nhs.net before the first transfer is undertaken. The channel **must** be encrypted. Arrangements where files contain Personal Data **must** complete a Data Privacy Impact Assessment before the first transfer is undertaken. Contact nhsbsa.dataprotection@nhs.net for further information. Data exchanges (even one-off events) **must** be subject to ISMSPOL 086 Data Protection and Confidentiality Policy. A Data Sharing Agreement **must** be produced, agreed and signed by all parties prior to any NHS data containing Personal Data or **OFFICIAL-SENSITIVE** data being passed or shared with any organisation or body external to NHSBSA.
NHSBSA managed Web Portals	Web Portals that are designed, created and managed by NHSBSA on behalf of wider NHS / DHSC e.g. MATEX	Content **must** be authorised by the head of service prior to submission for publishing **Must** be assured via the Security and Information Governance team at nhsbsa.informationsecurity@nhs.net prior to Go-Live All NHSBSA managed Web Portals **must** be compliant with OWASP Top 10.	Use of personal data prohibited unless encrypted (i.e. using HTTPS) and **must** be assured via the Security and Information Governance team at nhsbsa.informationsecurity@nhs.net All NHSBSA managed Web Portals **must** be compliant with OWASP Top 10.
Screens	Monitors / Computer Screens / Smart Walls / Hubs	Positioned or shielded to prevent viewing by non-employees	Positioned or shielded to prevent viewing by unauthorised parties. Possible measures include physical location in a secure area, privacy screen positioning of screen, use of password protected screen saver, etc.
	Public Display Screen Equipment	Content **must** be authorised by the head of service prior to submission for publishing	Prohibited

Data Source	Categories	OFFICIAL	OFFICIAL-SENSITIVE
File Storage		Files **should** be stored so that they can be viewed, modified or deleted within an official NHSBSA file-store by those users authorised to do so. Access management to an official NHSBSA file-store **must** be based on the Need-to-Know principle with assurance given from the nhsbsa.informationsecurity@nhs.net and authorised by the Information Asset Owner.	Files **must** be stored so that they can be viewed, modified or deleted within an official NHSBSA file-store by those users authorised to do so. The Files storage **should** be reviewed by Security and Information Governance and Security Architects to consider encryption requirement. Check with nhsbsa.informationsecurity@nhs.net for latest and acceptable encryption standards. Access management to an official NHSBSA file-store **must** be based on the Need-to-Know principle with assurance given from the nhsbsa.informationsecurity@nhs.net and authorised by the Information Asset Owner.
Printed Outputs		Printing of documents **should** be kept to a minimum and where only essential. Unattended printing is permitted only if physical access is used to prevent unauthorised persons from viewing the material being printed.	Printing of documents **must** be kept to a minimum and where only essential. Unattended printing is prohibited. Secure print **must** be enforced
End User Devices	Computers / Workstations	Password protected screen saver **must** be used when briefly unattended. To lock a screen, use the Windows and L Keys	Password protected screen saver **must** be used when briefly unattended. To lock a screen, use the Windows and L Keys
	NHSBSA Managed Laptops / Tablets / Smartphones	Full Hard Disk Encryption **must** be active. Password protected screen saver **must** be used when briefly unattended. To lock a screen, use the Windows and L Keys Hibernation or Shut down mode **should** be engaged when not in use or leaving work area. Kensington locks **should** be used to secure the device when leaving it at your desk. However, devices **must** be locked in a secure storage facility overnight Storing of data on your Desktop **should** be kept to a minimum	Full Hard Disk Encryption **must** be active. Password protected screen saver **must** be used when briefly unattended. To lock a screen, use the Windows and L Keys Hibernation or Shut down mode **should** be engaged when not in use or leaving work area. Kensington locks **should** be used to secure the device when leaving it at your desk. However, devices **must** be locked in a secure storage facility overnight Storing of data on your Desktop **must** be kept to a minimum
	Unmanaged Devices e.g. BYOD Laptops, Smartphones, etc that are not on the MDM	To be authorised by management	To be authorised by management

Data Source	Categories	OFFICIAL	OFFICIAL-SENSITIVE
Live Data in Development Environments		The use of Live data must be in line with the NHSBSA Secure Development Policy Assurance **must** be given from the Security & Information Governance team @ nhsbsa.informationsecurity@nhs.net before Live OFFICIAL data can be used within a Development Environment.	The use of Live data must be in line with the NHSBSA Secure Development Policy Prohibited, however Live OFFICIAL-SENSITIVE data may be anonymised or pseudonymised and or sanitised in line with the NHSBSA Anonymisation and Pseudonymisation Standard Prohibited unless an exception has been agreed with nhsbsa.informationsecurity@nhs.net before Live OFFICIAL data can be used within a Development Environment.
Live Data in Test Environments		The use of Live data must be in line with the NHSBSA Secure Development Policy Assurance **must** be given from the Security & Information Governance team @ nhsbsa.informationsecurity@nhs.net before Live OFFICIAL data can be used within a Development Environment.	The use of Live data must be in line with the NHSBSA Secure Development Policy Prohibited, however Live OFFICIAL-SENSITIVE data may be anonymised or pseudonymised and or sanitised in line with the NHSBSA Anonymisation and Pseudonymisation Standard Prohibited unless an exception has been agreed with nhsbsa.informationsecurity@nhs.net before Live OFFICIAL data can be used within a Test Environment.