NHS
Business Services Authority

Security Standard

Data Protection and Confidentiality Responsibilities

Issue sheet

Title	Data Protection and Confidentiality Responsibilities Standard v2.0
Author	Information Governance Manager
Owner	Head of Security and Information Governance
Issued to	NHSBSA DPO NHSBSA Caldicott Guardian NHSBSA Information Asset Owners
Reason issued	For action
Last reviewed	April 2023
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				Initial draft – pre-ISMS policy suite review.
1.1	February 2020	Information Governance Specialist	Information Governance Manager	Reviewed in light of changes to ISMS to ensure compliance with ISO27001 requirements.
2.0	February 2021	Information Governance Specialist	Information Governance Manager	Reformat cover page and removal of requirements section.

3.0	April 2023	Information Governance Specialist	Information Governance Manager	Annual Review

1. Introduction and Authorities

1.1 This document describes the Data Protection and Confidentiality Responsibilities Standard at the NHSBSA.

1.2 This standard gets its direct authority and approval from the Information Security Policy and supports and acts as a measure of compliance with the Data Protection and Confidentiality Policy. This Standard should be read in conjunction with these policies.

2. Audience

2.1 This standard is intended to be read and understood by all company employees, contractors, consultants, agency staff and Board members when acting in the capacity of Data Protection Officer, Caldicott Guardian, Information Asset Owner, or when dealing with personal or confidential information.

3. Scope

3.1 **Data Protection Officer (DPO)**

The DPO responsibilities include:

- All responsibilities detailed in the Information Security Responsibilities standard
- Carry out regular checks to monitor and assess new processing of personal data against the GDPR principles at the design as well as implementation points.
- Support the business to in carrying out Data Privacy Impact Assessments (DPIA) are carried out in compliance with GDPR requirements to effectively manage privacy risks relating to NHSBSA processing of personal data.
- Assure all Contracts, Data sharing agreements and Memorandums of Understanding comply with GDPR principles before sign-off. This will include ensuring that up to date best practice templates are available to staff for such agreements

- Ensuring compliance with individual's rights, including subject access, transparency, right to erasure, correction and objecting to processing by following the Information Rights Handling procedure.
- Referring any unmitigated high privacy risks to the SIRO.
- Ensuring the data protection ICO registration is renewed annually.
- Ensure the Caldicott Guardian receives suitable training and support to enable them to carry out their responsibilities.
- Liaise with the Caldicott Guardian regarding disclosures of patient identifiable data.
- Advise on the use of personal data outside the UK.
- Appropriately delegate responsibility to the Information Governance Team for any of these responsibilities.
- Objectively review any information right appeals in accordance with the Internal Review procedure.
- Act as a direct point of contact for Data Subjects.

3.2 Caldicott Guardian

The Caldicott Guardian's responsibilities include:

- Liaising and work with business area management and the NHSBSA Board in the course of promoting the Caldicott principles.
- Advising the Chief Executive and the NHSBSA Board on all aspects of processing patient-identifiable information including the implications of any concerns about processing patient identifiable data and present the board with options for improvement.
- Advising project leads on all aspects of the Caldicott principles, acting as an expert resource for them
- Ensuring only relevant staff can access sensitive patient data held within the designated Safe Haven within the Data Analytics Learning Laboratory.
- Reviewing and approve Safe Haven procedures applicable.
- Authorising all sharing of patient identifiable information and ensure such decisions are documented.
- Authorise the use of patient data outside the UK.
- Authorising any processing of patient identifiable information outside of England and ensure such decisions are documented.
- Bringing to the attention of the relevant manager any occasion where the appropriate procedures, guidelines and protocols may have not been followed.

- Delegate responsibility to the deputy Caldicott Guardian as appropriate

3.3 Information Asset Owners

All Information Asset Owners across the NHSBSA are directly responsible for:

- All responsibilities detailed in the Information Security Responsibilities Standard
- Ensuring that their staff are made aware of the content of any privacy notices and information processing agreements relevant to their role.
- Ensure that staff only access information on a need-to-know basis.
- Ensuring that staff recognise and respect all the information rights of customers and colleagues.
- Appropriately delegate these responsibilities to the Information Governance Team.

3.4 All NHSBSA Staff

All staff are directly responsible for:

- Meeting the responsibilities and principles detailed in the Information Security Responsibilities Standard
- Reporting any conflict of interest to their line manager when dealing with personal information. For example they know the customer/patient whose information they are processing.
- Maintaining the confidentiality of information. This means:
    - Only accessing person-identifiable or confidential information on a need-to-know basis.
    - Respecting the confidentiality of any confidential information disclosed to them
    - Not share any patient identifiable information unless it has been authorised by the NHSBSA Caldicott Guardian.
    - Not process any patient information outside the UK without the authority of the NHSBSA Caldicott Guardian.
- Ensuring that the information they capture is as accurate as possible.
- Ensuring that personal data is securely disposed of in accordance with the NHSBSA Destruction Standard when it is no longer required.
- On receipt of a request to use an information right about their personal data that is outside their “Business As Usual” processes, immediately notify the

Information Governance team and their line manager. Information rights requests include:

- a copy of the information we hold about them
- Have their records deleted, erased or forgotten
- Objecting to our processing their information
- Disputing the accuracy of the information
- Details of a breach of their information rights by NHSBSA or anyone acting on our behalf

- Making sure that on receipt of a request from a public sector organisation for the personal details of individual(s) liaise with the Information Governance Team to confirm how these should be authorised.
- Being aware that it is a criminal offence to:
  - alter, deface, block, erase, destroy or conceal any personal data to prevent disclosure which is held by NHSBSA.
  - to seek to re-identify individuals from anonymised information without authorisation by the NHSBSA.
  - To steal Personal data, for example keeping personal data they had access to in their role after leaving the NHSBSA
- Recognising that when NHSBSA provides customers or staff with a copy of their information that staff personal details will be disclosed where the customer has had direct and identifiable communications with them; unless one of the statutory exemptions/exceptions applies. The principle regarding the disclosure of staff details to the public is stated in the Freedom of Information Policy
- All NHSBSA employees involved in changing how personal data is processed will:
  - Involve the Information Governance Team at an early stage in assessing the impact of any changes in the use of personal data including Data sharing and transfers.
  - Ensure any changes to the use of personal data are signed off by the Information Governance Team before processing starts.

4. References

4.1 The NHSSBA comply with the legal and professional obligations set out in :

- The Data Protection Act 2018
- General Data Protection Regulation 2016
- Common Law Duty of Confidence
- NHS Act 2006 requirements concerning confidentiality