NHS
Business Services Authority

Corporate policy

Data Protection and Confidentiality Policy

Issue sheet

Document reference	NHSBSADPN001d
Document location	S:\BSA\IGM\Mng IG\Developing Policy and Strategy\Develop or Review DPA Policy\Current and Final
Title	NHS Business Services Authority Data Protection and Confidentiality policy
Author	Chris Gooday
Issued to	All BSA staff on hub, published publicly on website
Reason issued	For information / action
Last reviewed	Sept 2017
Review cycle	Annual
Date of Equality Assessment	N/A
Date of Fraud Review	N/A

Revision details

Version	Date	Amended by	Approved by	Details of amendments
Initial release	30.05.2007	-	IGSG	This policy covers corporate directorates as well as the business areas of the Operations directorate. The IGSG requires that this is made clearer in the policy, specifically at points 6.6 and 6.7.
a	08.07.2008	Gordon Wanless	IGSG	Changed “Telecommunications Act 1984 and 1997 amendments” to be “Communications Act 2003”, along with associated explanatory text. Changed “HSG (96)18 The Protection & Use of Patient Information” to be “Confidentiality: NHS Code of Practice”, along with associated explanatory text Changed “MG:E5498 Ensuring Security and Confidentiality in NHS

				Organisations" to be "Information Security Management: NHS Code of Practice", along with associated explanatory text Changed "HSC 2002/003 Implementing The Caldicott Standard into Social Care" to be "The Caldicott Guardian Manual 2006", along with associated explanatory text Changed "BS7799 Industry and adopted NHS IT security standard" to be "Information Commissioner's Guidance – Use and Disclosure of Health Data", along with associated explanatory text
b	3.11.2010	G Wanless	IGSG	Added details of DP deputies
c	29.09.2013	G Wanless	A&PF	Amend roles and responsibilities in section 6.6
d	28.02.2014	C Gooday	A&PF	1.1 Reflect NHS Restructure 2013 names, 1.6 Equalities Act 2010 supersedes race Relations and Sex Discrimination Acts 1.7 Reflect Caldicott 2 guidance changes and SAR Code of Practice 1.7 change of Job title
E	15.11.2017	C Gooday	A&PF	Update to reflect GDPR obligations, merged with Caldicott and Safe Haven Policies and restructured to meet requirements of ISMS

1. Policy Summary

1.1. This policy sets out roles and responsibilities when personal data is being processed to ensure the rights and privacy of individuals are respected.

2. Introduction

2.1. The NHSBSA needs to obtain and process information about different people for many purposes. These are detailed in the Data Protection regulator's public register NHSBSA entry here.

2.2. The NHS Business Services Authority (NHSBSA) has a legal obligation to comply with all appropriate legislation in respect of data protection and patient confidentiality principles. It also has a duty to comply with guidance issued by NHS England, NHS Digital, Health Research Authority and other advisory groups to the NHS and guidance issued by professional bodies.

3. Scope

3.1. This policy applies to all employees, Non-executive Directors, contractors, agents, representatives and temporary staff working for or on behalf of the NHSBSA. These will be referred to as Staff in the remainder of this policy.

3.2. The policy applies to all information falling within the GDPR definition of personal data. This means information that relates to living individuals that can by identified or singled out directly or indirectly by anyone. Individuals can be identified by various means including, name, address, an identification number, location data, and an online identifier such as cookies or IP address or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

3.3. This policy applies to all personal information processed including:

- Manual records such as paper and microfiche.
- Electronic records such as Computer and Cloud records, CCTV and Telephone recordings
- Any extracts taken, printed, copied, transferred or verbally connected with the activities of the NHSBSA.

3.4. Anonymised or aggregated data is not within the scope of GDPR, provided it is reasonably unlikely that the anonymisation or aggregation can be reversed. Therefore it falls outside the scope of this policy. The NHSBSA Anonymisation and Pseudonymisation Standard determine how personal data will be anonymised.

4. Objectives

4.1. The objectives of this policy are:

- To ensure the reputation of the NHSBSA is upheld with respect to customers and staff information rights. This will prevent this being a barrier to providing or managing new public services.
- To enable the sharing of personal data with other organisations to help provide insight into how to better plan NHS services.
- To avoid enforcement action for breaching data protection legislation requirements.
- To ensure compliance with all Information Governance law including the General Data Protection Regulation EU 2016/679 (GDPR)

5. Key outcomes (or Expected Results)

5.1. NHSBSA will respect the information rights of customers and staff and thereby maintain a good reputation with customers, staff and stakeholders regarding its handling of the large volume of personal information it processes.

5.2. NHSBSA will be trusted by Data Sharing Agreement partners when handling personal data and continue to use this information to provide insight to assist in planning NHS Services.

5.3. NHSBSA will avoid regulatory enforcement action, together with the associated complaints, negative publicity, the cost of changing work practices and possible fines and compensation claims.

6. Principles

6.1. NHSBSA aims to be open and transparent when processing and using personal and sensitive data by ensuring we follow the Data Protection Principles of good data handling as described in Article 5 of the GDPR:

- Compliance with the following three principles will be delivered through the privacy by design procedure:
  - Lawfulness, Fairness and Transparency,
  - Purpose Limitation
  - Data Minimisation

- The Accuracy principle will be met by the Data Governance Framework.

- The Storage limitation will also be addressed in the Records Management Policy and by adherence to the Anonymisation and Pseudonymisation Standard.

- Compliance with the Integrity and Confidentiality principle is detailed in the Information Security Policy.

6.2. Staff personal information will be disclosed when the NHSBSA provides customers or staff with a copy of their information where the customer has had direct and identifiable communications with them; unless one of the statutory exemptions/exceptions applies.

6.3. The principle regarding the disclosure of staff details to the public is stated in the Freedom of Information Policy.

6.4. The Caldicott Principles will be complied with when handling patient identifiable information.

7. Responsibilities

7.1. Data Protection Officer

The Data Protection Officer responsibilities include:

- All responsibilities detailed in the Information Governance Policy
- 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.
- Ensure that Data Privacy Impact Assessments (DPIA) are carried out at an early stage of any change 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 ICO.
- Ensuring the data protection ICO notification is reviewed, maintained and renewed annually for all use of personal information.
- 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 or the processing of that data outside England.
- 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.

7.2. **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.
- 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.

7.3. **Information Asset Owners**

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

- All responsibilities detailed in the Information Governance Policy
- 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.

7.4. **All Staff**

All Staff are directly responsible for:

- Meeting the responsibilities and principles detailed in the Information Governance Policy

- 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 England 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.

8. Related policies

8.1. This policy follows:

Information Governance Policy

8.2. The following rely on this policy when personal data is being processed:

Records Management Policy
Information Security Policy
Freedom of Information Policy

9. Penalties

9.1. Any user who violates this Data Protection and Confidentiality Policy document will be subject to disciplinary action.