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 |
| Owner | Marc Compton |
| Issued to | All NHSBSA staff on hub, published publicly on website |
| Reason issued | For information / action |
| Last reviewed | December 2020 |
| 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. |
| 1.0 | 08.07.2008 | Gordon Wanless | IGSG | Changed “Telecommunications Act 1984 and 1997 amendments” to be “Communications Act 2003”, along with associated explanatory text.<br><br>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<br><br>Changed “HSC 2002/003 Implementing The Caldicott Standard into Social Care” to be “The Caldicott Guardian Manual 2006”, along with associated explanatory text<br><br>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 |
| 2.0 | 3.11.2010 | G Wanless | IGSG | Added details of DP deputies |
| 3.0 | 29.09.2013 | G Wanless | A&PF | Amend roles and responsibilities in section 6.6 |
| 4.0 | 28.02.2014 | C Gooday | A&PF | 1.1 Reflect NHS Restructure 2013 names,<br>1.6 Equalities Act 2010 supersedes race Relations and Sex Discrimination Acts<br>1.7 Reflect Caldicott 2 guidance changes and SAR Code of Practice<br>1.7 change of Job title |
| 5.0 | 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 |
| 6.0 | 08.12.2020 | C Gooday | A&PRF | Revised issue sheet and move roles and responsibilities to a standard and feedback from Caldicott Guardian |

## 1. Policy Summary

1.1. This policy sets out the policy principle statements applicable when personal data is being processed to ensure the rights and privacy of individuals are respected and treated in accordance with data protection legislation.

## 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 including the Caldicott principles. It also has a duty to comply with guidance issued by NHS England, NHS Digital, Health Research Authority, National Data Guardian 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. In addition, the policy applies to information relating to deceased patients.

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, and Metadata.
- 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 and reputational damage, 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 data protection impact assessment procedure:
  - Lawfulness, Fairness and Transparency,
  - Purpose Limitation
  - Data Minimisation
- The Accuracy principle will be met by the Data Governance Policy.
- 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. Related policies

7.1. This policy follows:

Information Security Policy

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

Records Management Policy
Freedom of Information Policy

## 8. Penalties

8.1. Any Staff who violate this policy will be subject to disciplinary action up to and including dismissal, and criminal prosecution.