NHS
Business Services Authority

Corporate policy

Information Governance Policy

Issue sheet

Document reference	NHSBSAIGM002a
Document location	S:\BSA\IGM\Mng IG\Developing Policy and Strategy\Develop or Review IG Policy\Current and Final
Title	NHS Business Services Authority Information governance policy
Author	Gordon Wanless
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	
Date of Fraud Review	

Revision details

Version	Date	Amended by	Approved by	Details of amendments
Initial release	31.05.2007	-	**IGSG**	The third last bullet point in 3.1.1 to include reference to EIR and PSI. Amend “affordable” in the last bullet point in 3.1.1 to be “cost-effective”. The fourth bullet point in 3.1.2 to include reference to EIR and PSI. Add “within cost and resource restraints” at the end of the third bullet point in 3.1.4.
a	16.01.2014	C Dunn & C Gooday	IGSG	Amendments to reflect PCI DSS Compliance 3.2 Review period changed from periodically to annually
b	18.01.2018	C Gooday	GDPR Project Board	Update to reflect GDPR obligations, and restructured to meet requirements of ISMS

1. Policy Summary

1.1. This policy specifies how the NHSBSA manages all information to meet legal and sector specific obligations.

2. Introduction

2.1. The information held by the NHS Business Services Authority (NHSBSA) represents one of our most valuable assets. Without that information the NHSBSA could not operate. It is therefore essential that all information and information systems at the NHSBSA's sites are protected against the many threats which may affect confidentiality, integrity, availability, resilience and overall service provision. and reputation. Such threats can range from accidental damage to deliberate disclosure of sensitive information.

2.2. The NHS Business Services Authority (NHSBSA) has a legal obligation to comply with all appropriate legislation in respect of Information Governance principles. It also has a duty to comply with guidance issued by NHS England, NHS Digital, 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 and non-NHSBSA employees such as 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 recorded information held by or on behalf of the NHSBSA, including, but not limited to:

- members of the public
- non-NHSBSA employees
- Staff
- organisational, business and operational information
- Cardholder data.

3.3. This policy applies to all aspects of information handling, including, but not limited to:

- information recording and processing systems whether manual or electronic,
- information transmission systems, such as fax, e-mail, portable media, post and telephone.
- Information disclosures and sharing
- Awareness / reference materials and presentations

3.4. This policy covers all information systems purchased, developed and managed by / or on behalf of, the NHSBSA.

4. Objectives

4.1. The objectives of this policy are to ensure the confidentiality, integrity and availability of NHSBSA information by ensuring the data is:

- Held securely and confidentially
- Obtained fairly and lawfully
- Recorded accurately and reliably
- Used effectively and ethically
- Shared and disclosed appropriately and lawfully

4.2. This will be measured by the annual NHS Information Governance toolkit return.

5. Key outcomes (or Expected Results)

5.1. NHSBSA will use the information it holds to most effectively meet strategic goals including supporting the NHS within Information Governance constraints.

5.2. NHSBSA will be trusted by stakeholders, customers and staff when processing very large volumes of information.

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

6. Principles

6.1. NHSBSA has developed a framework for this policy. This is supported by a set of Information Governance policies and related procedures to cover all aspects of Information Governance which are aligned with the NHS Information Governance toolkit requirements.

6.2. The Key Information Governance Policies are:

Policy	Purpose
Information Security Policy	The purpose of this policy is to protect the confidentiality, integrity,availability and resilience of all information. The policy defines security measures applied through technology and appropriate procedures.
Acceptable Use Policy	The aim of the policy is to ensure that staff are given the relevant support to ensure they are aware of what is acceptable use of

	any computer system owned or operated by the NHSBSA and therefore can apply procedures accordingly.
Data Protection and Confidentiality Policy	This policy sets out roles and responsibilities when personal data is being processed to ensure the rights and privacy of individuals are respected, ensuring compliance with current Information Rights legislation.
Freedom of Information Policy	This policy sets out the roles and responsibilities for compliance with the Freedom of Information Act and Environmental Information Regulations.
Records Management Policy	This policy promotes the effective management and use of information, recognising its value and importance as a resource for delivering NHSBSA objectives
Business Continuity / Disaster Recovery Policy	This policy: • ensures that all Business Continuity Management (BCM) activities are conducted and implemented in an agreed and controlled manner • ensures that the NHSBSA achieve a business continuity capability that meets changing business needs and is appropriate to the size, complexity and nature of the NHSBSA • puts in place a clearly defined framework for the on-going BCM capability

6.3. Policies will not duplicate content but rather refer to the policy which covers overlapping content.

6.4. The terms used in these policies will be documented in the ISMS definitions document.

6.5. A risk based approach will be taken with regard to the nature, scope, context and purposes of the information being processed.

7. Responsibilities

7.1. The Chief Executive.

The Chief Executive has overall responsibility for strategic and operational management, including ensuring that NHSBSA policies comply with all legal, statutory and good practice guidance requirements.

The Chief Executive, whilst retaining legal responsibility has delegated Information Governance compliance to the Data Protection Officer (DPO).

The Chief Executive will ensure that the DPO is not pressurised by the organisation as to how to perform their tasks, and is protected from disciplinary action when carrying out tasks specified in Information Rights legislation.

7.2. The Senior Information Risk Owner.

The Senior Information Risk Owner (SIRO) is the Executive Director of Corporate Services and Corporate Secretary and therefore part of the NHSBA Board, who will:

- Be accountable for information risk within the NHSBSA and advise the Board on the effectiveness of information risk management across the organisation.
- Delegate operational responsibility for Information Security to the NHSBSA Head of Security and Information Assurance
- Ensure that all Information Security risks are managed in accordance with the NHSBSA Risk Management Policy.
- Provide written advice to the Chief Executive on the content of the organisation's statement of internal control in regard to information risk.
- Receive training as necessary to ensure they remain effective in their SIRO role.

7.3. Data Protection Officer

The Data Protection Officer (DPO) responsibilities have been allocated to the Head of Information Governance role within the NHSBSA. The DPO reports to the SIRO. This ensures the DPO can act independently, without a conflict of interest and report direct to the highest management level. In addition the DPO will Deputise for the SIRO and Caldicott Guardian.

The Data Protection Officer is responsible for ensuring that the NHSBSA and its constituent business areas remain compliant at all times with Data Protection,

Privacy & Electronic Communications Regulations, Freedom of Information Act and the Environmental Information Regulations (Information Rights legislation).

The Data Protection Officer shall:

- Lead on the provision of expert advice to the organisation on all matters concerning the Information Rights Law, compliance, best practice and setting and maintaining standards.
- Provide a central point of contact for the Information Rights Legislation both internally and with external stakeholders (including the Office of the Information Commissioner).
- Communicate and promote awareness of Information Rights Legislation across the NHSBSA.
- Lead on matters concerning individual's right to access information held by NHSBSA and the transparency agenda.
- Act as the Freedom of Information Officer regarding Information Access legislation as detailed in the Freedom of Information Policy.

The DPO responsibilities include:

- Ensuring that appropriate Information Rights legislation policies for the NHSBSA are produced and kept up to date.

- Ensuring that the appropriate procedures and practices are formulated and adopted in an effective framework for the management of Information in compliance with Information Rights legislation by the NHSBSA.

- Report to the Board on the NHSBSA's level of Information Rights legislation compliance and associated risks.

- Setting the standard of Information Rights legislation training for staff across the NHSBSA.

- Monitor and audit compliance with Information Rights legislation related policies.

- Maintaining an expert knowledge of data protection matters and a detailed understanding of the organisations business and purposes.

- Support the Leadership Team and SIRO by ensuring the availability and provision of relevant professional advice on information governance issues, with the exception of Information Security.

- Provide appropriate assurances to the Senior Information Risk Owner (SIRO) to allow the SIRO to provide appropriate assurance the Accountable Officer.
- Delegate the above responsibilities, as appropriate, to the Information Governance Team.

- Ensure that the Information Governance team reporting to the DPO is adequately resourced to meet the NHSBSA's legal obligations.

- Ensure the NHSBSA has adequate, up-to-date and tested business continuity arrangements across all its services.

7.4. Caldicott Guardian

The Caldicott Guardian is responsible for ensuring implementation of the Caldicott Principles and Data Security Standards with respect to Patient Confidential Data. The Caldicott Guardian has been allocated to the Chief Insight Officer. The DPO shall deputise for the Caldicott Guardian.

The responsibilities of the Caldicott Guardian are detailed in the Data Protection and Confidentiality Policy.

7.5. Head of Security and Information Assurance

The Head of Security and Information Assurance (HSIA) is responsible for the day to day operational effectiveness of the Information Security Policy and its associated policies and processes.

The HSIA shall:

- Lead on the provision of expert advice to the organisation on all matters concerning information security, compliance with policies, setting standards and ensuring best practice.
- Provide a central point of contact for information security.
- Ensure the operational effectiveness of security controls and processes.
- Monitor and co-ordinate the operation of the Information Security Management System.
- Be accountable to the SIRO and other bodies for Information Security across the NHSBSA.
- Monitor potential and actual security breaches with appropriate expert security resource.

7.6. The Information Governance and Security Group.

An Information Governance and Security Group will oversee the development and implementation of data and Information Governance in the NHSBSA and ensure

that the NHSBSA complies with legal requirements, the NHS Mandatory Information Governance Framework and best practice. This group includes the SIRO, DPO, HSIA and Caldicott Guardian.

Its responsibilities include:

- Act as an escalation point for Information and Data Governance risks and issues.
- Monitor business changes that introduce Information Governance risk.
- Co-ordinate the work to resolve Information and Data Governance risks and issues.
- Review and sign off any Information Governance reports to the Board.

7.7. **Information Asset Owners**

The Information Asset Owners are senior/responsible individuals involved in running the business area. All Information Asset Owners across the whole of the NHSBSA are directly responsible for:

- Understanding what information is held
- Knowing what information is added and removed
- Understanding how information is moved
- Knowing who has access to the information and why
- Ensuring that their staff are aware of their Information Governance responsibilities.
- Ensuring that their staff have completed suitable Information Governance training.
- Ensuring that this policy and its supporting standards and guidelines are built into local processes
- Ensure that audits and spot checks are carried out quarterly to ensure staff adhere to Information Governance policies. This includes knowing who has access to the information and why.

- Promptly report any breaches of Information Governance policies using the Information Security Reporting Procedure.

- Delegate these responsibilities, as appropriate, to their staff.

7.8. **All Staff**

All staff are responsible for:

- Only processing information as defined by NHSBSA procedures and standards.

- Completing training relating to Information Governance policies within the timescales communicated to them including annual mandatory refresher training.

- Information security and the appropriate protection of information assets .They remain accountable for their actions in relation to NHS and other UK Government information and information systems.

Staff **shall** ensure that they understand their role(s) and responsibilities.

8. Related policies, standards and procedures.

8.1. All Information Governance policies rely on this policy.

9. Penalties

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