

A thick blue horizontal bar with a slight upward curve in the center, spanning the width of the page.

Statistics at NHSBSA
Confidentiality and Access Statement

Document Release Note

Document Name: Confidentiality and Access Statement

Document Details Name	Version Number	Description
Confidentiality and Access Statement	v002	A corporate document outlining the NHSBSA's confidentiality and access statement for Official Statistics

Revision Details Revision Number	Revision Date	Revision Description	Page Number	Previous Page Number	Action Taken	Addenda/ New Page
v002	24/04/2021	Updated as part of annual refresh			Minor typographical changes	

About this document

This is the NHS Business Services Authority's (NHSBSA) policy and procedure on confidentiality and access in relation to the production of Official and National Statistics.

Table of Contents

Section 1: Introduction.....	4
Section 3: Staff.....	4
Section 3: Physical Security	4
Section 4: Technical Security	5
Section 5: Organisational Security	5
Section 6: Statistical Disclosure Control.....	5

Section 1: Introduction

The NHS Business Services Authority (NHSBSA) as a producer of Official Statistics is committed to adhering to the responsibilities set out in the Code of Practice for Official Statistics around confidentiality and data governance (T6: Data Governance). The NHSBSA is also governed by the organisation's own data protection and confidentiality policy along with General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018.

This statement describes the policies, processes, structures and roles that are in place to ensure that the NHSBSA upholds the confidentiality of the individuals that it holds data for when producing Official Statistics. Further details are set out in the following documents, and other documents that they reference in turn:

- [Information governance policy](#)
- [Information security policy¹](#)
- [Data handling and storage policy](#)
- [Data protection and confidentiality policy](#)
- [Information security incident management standard procedure](#)
- [Home working computer security policy](#)
- [Mobile computing policy](#)
- [End user computing policy](#)
- [Statistical Disclosure Control policy](#)

Each of these documents contains a clear revision history and is subject to an annual review. They may be updated more frequently in response to changes in legislation and or best practice. Contact details for the team responsible for each of these policies can be found within the documents themselves.

Section 2: Staff

All NHSBSA staff who access and process data about individuals are given training on their obligations under all relevant legislation and all internal information security and governance policies. This training is refreshed annually.

Section 3: Physical Security

All NHSBSA staff have roles and responsibilities set out in our information security policies that set out physical security requirements, standards and procedures.

¹ This is an umbrella policy that references all related Information Security policies within our Information Security Management System (ISMS), and is aligned to ISO27001 and ISO27002.

These include the Information security policy, the data handling and storage policy, the home working computer security policy and the mobile computing policy

Section 4: Technical Security

The NHSBSA information security policy referred to in section one sets out requirements that safeguard our information assets in terms of technical requirements for:

- user access controls
- application access control
- computer and network procedures
- Security incidents and weaknesses
- Protection from malicious software
- Removable media
- System change

Section 5: Organisational Security

The people who fulfil the following roles, set out in our Information governance policy or where noted below, have specific responsibility for information security and protection of personal privacy at the NHSBSA:

- Senior Information Risk Owner (SIRO) – Executive Director of Corporate Services
- Data Protection Officer (DPO) – Information Governance Manager.
- Caldicott Guardian – Executive Director of Strategy, Business Development and Growth.
- Head of Security and Information Assurance (HSIA)
- Business Information Security Group (BISG) – set out the Information security policy

There are also Information Asset Owners throughout the business responsible for their own areas.

Section 6: Statistical Disclosure Control

We apply statistical disclosure control where we have deemed there is a reasonable risk of identifiable personal information being released or inferred from a release of a statistical product. This risk is determined by an internal risk assessment process that is documented with all statistical products. Where a risk has been identified a method of disclosure control will be used to reduce this risk of disclosure while minimising impact on the utility of the statistics.

For more information please see our disclosure control protocol which is published separately.

Contact us

Feedback is important to us; we welcome any questions and comments relating to this document.

Please quote 'Confidentiality and Access Statement' in the subject title of any correspondence.

You can contact us by:

Email: nhsbsa.statistics@nhs.net

Telephone: 0191 203 5050

You can also write to us at:

NHSBSA - Statistics
NHS Business Services Authority
Stella House
Goldcrest Way
Newburn Riverside
Newcastle upon Tyne
NE15 8NY

END.