Safe haven policy

Issue sheet

Document reference	NHSBSADPN006a
Document location	S:\BSA\IGM\Mng IG\Developing Policy and Strategy\Develop or Review of IS Policy\Current and Final
Title	NHS Business Services Authority Safe Haven Policy
Author	Gordon Wanless
Issued to	All staff
Reason issued	For action

Revision details

Version	Date	Amended by	Approved by	Details of amendments
Initial release	21.09.2009	-	IGSG	
a	19.05.2014	C Dunn		Section 3. Change of wording to HoIG
b	24.3.15	C Gooday	APF	Annual Review
c	21.3.16	C Gooday	APF	Annual Review

Contents

1.   Introduction

1.1   Safe haven is a term used to explain an agreed set of arrangements that are in place in an organisation to ensure confidential person identifiable information (e.g. patients and staff information) can be communicated safely and securely.

1.2   All NHS organisations need to have a safe haven policy to ensure the privacy and confidentiality of information and to adhere to the legal restrictions placed on them, especially concerning sensitive information (e.g. people's medical condition).

1.3   There is a need for NHS organisations to document the procedures they have in place to ensure confidential information is only accessed by relevant staff.

1.4   The Caldicott Guardian for the organisation must approve this policy.

2.   Objectives, aim and scope

2.1   The objective of this policy is to document what procedures the NHSBSA has in place to discharge its safe haven duties.

2.2   The aim of the policy is to ensure that staff are given the relevant support to ensure they are aware of the requirements of safe haven and apply procedures accordingly.

2.3   This policy applies to all business areas of the NHSBSA.

3.   Responsibilities

Overall responsibilities

3.1   Ultimate responsibility for this Policy rests with the NHSBSA Leadership Team, but on a day-to-day basis the Information Governance and Security Group (IGSG) and the NHSBSA Head of Internal Governance (HoIG) role within the NHSBSA will be responsible for managing and implementing the policy.

Head of Internal Governance

3.2   HoIG responsibilities include:

- To ensure that the designated training system for training in the areas of data protection and information security covers the Safe Haven requirements.

- To develop, maintain and effectively cascade an NHSBSA-wide Data Classification Matrix that assists staff to send confidential person identifiable information in an appropriately secure manner.

Internal audit

3.3   The NHSBSA will regularly audit its practices for compliance with this policy.

The audit will:

- identify areas of operation that are covered by the NHSBSA's policies and identify which procedures and/or guidance should comply to the policy
- follow a mechanism for adapting the policy to cover missing areas if these are critical to the management of mobile computing, and use a subsidiary development plan if there are major changes to be made
- set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance
- highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures.
- The results of audits will be reported to the IGSG.

4.   Validity of this policy

4.1   This policy is designed to avoid discrimination and be in accordance with the Human Rights Act 1998 and its underlying principles.

4.2   This policy should be reviewed annually under the authority of the NHSBSA Leadership Team.