

THE NEWCASTLE UPON TYNE HOSPITALS NHS FOUNDATION TRUST

Reporting of Data Security/Confidentiality Breaches

Effective from: May 2007

Review date: May 2010

1. Introduction

1.1 The purpose of this procedure is to provide guidance for all Trust employees about the reporting of data security/confidentiality breaches.

2. Definition

2.1 For the purposes of this procedure a breach is defined as follows:

‘A breach of data security/confidentiality is an action or event that alters the integrity of, or causes the unauthorised disclosure of any information relating to the Trust or its business including Personal Identifiable Information to a third party. Disclosure can be oral or written, by telephone, fax or electronic media including e-mail or health information networks. All personal identifiable information held within the organisation is subject to the Data Protection Act 1998, Human Rights Act 1998, the Computer Misuse Act 1990, the Caldicott Principles and Trust Information Security Policies’.

2.2 Examples of a breach include:

- (i) Accessing a patient record (paper or computerised) when you are not part of the care team.
- (ii) Discussing patient information in a public area, e.g. canteens.
- (iii) Discussing patient information where staff who are not part of the care team may overhear e.g. hopper, lifts.
- (iv) Leaving a Personal Computer with patient information displayed in an area where the public or staff not involved with the patient may see the information.
- (v) Transmitting patient information by e-mail to a non-NHS e-mail account.
- (vi) Transferring patient identifiable information by portable media (e.g. memory stick) when not authorised to do so by the Caldicott Guardian.

3. Responsibility

3.1 It is the responsibility of all Trust employees to ensure that they do not commit data security/confidentiality breaches. **Any reported breach shall be investigated and, where appropriate, disciplinary or legal action**

taken. It is also the responsibility of all Trust employees to report data security/confidentiality breaches should they become aware of, or suspect, such a breach.

4. Reporting of data security/confidentiality breaches

4.1 Should an employee become aware of, or suspect, a data security/confidentiality breach they ought to report the breach, or suspected breach, to the Trusts Information Management & Technology Security Manager. Contact can be made by telephone on extension 37368 or e-mail Richard Oliver.

The e-mail address to be used to contact the IM&T Security Manager is Richard.Oliver@nuth.nhs.uk.

4.2 The IM&T Security Manager shall be responsible for investigating reported data security/confidentiality breaches and deciding what action to take. The IM&T Security Manager will notify the Head of Information & Management Technology about their activities.

4.3 The Trust's IM&T Panel shall receive quarterly reports from the IM&T Security Manager about the number of reported data security/confidentiality breaches, follow-up actions taken and trend analysis. The sensitive nature of the information concerned shall be taken into consideration when quarterly reports are produced.

5. Further Information

5.1 Further details concerning the Trusts approach to information security can be found within the Information Security Policy via the Policies and Procedures section of the Trust Intranet.

6. Review

The Personnel Manager is responsible for the review of this procedure.