

Incident Reporting Policy

Effective April 2010

Review March 2013

1 Introduction

- 1.1 The Trust has a responsibility to monitor all information incidents that occur within the organisation that may breach security and/or confidentiality of personal information. The Trust also needs to ensure that all incidents are identified, reported and monitored. The Trust already has a method of recording clinical incidents but not necessarily information incidents relating to breaches of security and confidentiality.
- 1.2 The document attempts to detail the process of identifying, recording and monitoring information incidents. This is a requirement of the Caldicott recommendations and ISO17799.

2 What is an information incident?

- 2.1 An information incident relating to breaches of security and/or confidentiality could be anything from users of computer systems sharing passwords to a piece of paper identifying a patient being found in a public place.
- 2.2 A security incident might be a 'usual' everyday event e.g. accidentally entering the wrong password or the wrong user id, forgetting to change a password within a specified time period.
- 2.3 A security incident might be an 'unusual' event e.g. something odd happening on the screen, a computer file disappearing, an unaccompanied stranger in a restricted area.
- 2.4 An IM&T security incident is defined as any event that has resulted or could result in:
- The disclosure of confidential information to any unauthorised person
 - The integrity of the system or data being put at risk
 - The availability of the system or information being put at risk
 - An adverse impact e.g.
 - Embarrassment to the NHS
 - Threat to personal safety or privacy
 - Legal obligation or penalty
 - Financial loss
 - Disruption of activities
- 2.5 All incidents should be reported to the immediate line manager and the Trust IT Security Officer.
- 2.6 A virus incident should be reported to the IT Service desk. The service desk will then notify the IT Security Officer and IT technical staff as per the Virus Notification procedure. **Appendix 1**

2.7 Some incidents may impact on other parts of the NHS e.g. a virus and if this is the case the incident should be reported to the NHS Information Authority Security and Data Protection Officer. A separate Virus incident reporting form will be completed and actioned by the IT Security Officer.

2.8 Some examples of these types of incidents include:

- A computer printout of patient details being printed at the wrong printer.
- Finding a clinic list, the back of which is used for a shopping list, in the supermarket
- Finding a patient manual record in a ladies toilet within a hospital site
- Finding a patient record in the back of an unattended wheelchair used by porters to move patients
- Identifying that a fax that was thought to have been sent to a GP had been received by a private householder
- Giving out identifiable information about an individual over the telephone
- Losing a laptop computer with personal information on it
- Giving information to someone who should not have access to it – verbally, in writing or electronically
- Accessing a computer database using someone else's authorisation e.g. someone else's user id and password
- Trying to access a secure area using someone else's swipe card or pin number when not authorised to access that area
- Finding your PC and/or programmes aren't working correctly – potentially because you may have a virus
- Software malfunction
- Sending a sensitive e-mail to 'all staff' by mistake
- Finding an employee's password written down on a 'post-it'
- Finding someone has tried to 'break in' to the office/building

3 How should this be reported?

3.1 All employees (contracted and non-contract) should be made aware through their contract of employment, training and by their manager of what is considered to be an incident.

3.2 They should be made aware that if they discover something that could be considered as an incident they should report this to their manager and complete an incident form available from general office

3.3 The IT Security team should be informed of the incident with the incident number from the form noted.

3.4 The form, which should be numbered, should identify the following:

- Date of discovery of incident
- Place of incident
- Who discovered incident
- Details of incident
- Category/classification of incident
- Report to senior management if risk to organisation and/or patient care

- Any action taken by person discovering incident at time of discovery
- Date incident reporting form has been sent to the IT Security Officer.
- Action taken by security officer to ensure incident does not occur again
- Follow-up action to check no re-occurrence of incident

4 How should these be responded to?

- 4.1 The IT Security Officer should be informed of the incident and will forward details to Data Protection Officer and the Caldicott Guardian if the incident pertains to patient information.
- 4.2 The risk management team should log the incident to enable a central register to be maintained of all incidents occurring within the organisation.
- 4.3 All registered incidents should be re-evaluated after a 6 month period to ensure the type of incident is no longer being reported or the volume of those types of incidents has dramatically reduced.
- 4.4 If there is no change in the volume of each type of incident the senior management should be alerted and appropriate action taken. This could be further training courses for staff or an improvement to existing security and/or confidentiality arrangements.
- 4.5 Some incidents may involve the invoking of the Trust Disciplinary Procedures. Incidents that are deemed to be a disciplinary offence are detailed within the Disciplinary Procedures.
- 4.6 Staff should refer to the Incident Management Policy on the Trust Intranet.
<http://intranet/Policies/corporategov/Incident%20Management.PDF>

Author: Director of Information Technology.

Virus Notification

Introduction

This document outlines the methods for the notification, containment, reporting and prevention of virus attacks.

There are many ways a virus can find it's way onto a PC, the most common ways are; via an e-mail (with attachment), running an unchecked program downloaded from the Internet, or using an infected floppy disk or CD.

Resource

The IT Security Team – Matt Carney & Alan Richardson

The Network Manager – Bob Beckwith, and the Network Support staff, Helpdesk staff.

Frequency

This procedure should be followed every time a virus infection is suspected or identified.

Responsibility

It is the responsibility of all the members of the IT Department to follow this procedure. Either the IT Security Team, or the Network Manager in their absence, must report a major virus incident, to David Harley at NHS Information Authority.

Notification

When a PC on the Trust's Network becomes infected, a virus notification e-mail will be sent to:

- IT Security Team.
- IT Network Officers.
- Helpdesk.

The e-mail will outline the virus, usually containing the following information:

- Name of virus.
- Which file it has infected.
- Name of the infected PC.
- IP address of the PC.
- The username of the person that's currently logged onto the PC.
- An action i.e. cured, deleted, re-named, no action.

Two examples of the virus notification e-mail can be seen below.

- a) The Win95/Marburg.8590.A Virus was detected in C:\WINDOWS\notepad.exe. Machine:F_WARD_12, Address: 160.160.121.6, User:ward_12, Action:CURE.
- b) The Win32/Klez.H.Worm Virus was detected in C:\PROGRAM FILES\COMPUTERASSOCIATES\INOCULATEIT\VIRUS\VIRTUAL.ASP.EXEM achine:F_A_MCCALL, Address: 160.160.121.64, User:enamc, Action:DELETE.

Containment

The response to the virus notification e-mail depends on the virus type, the level of impact to the Trust and the action performed by the virus checker. These can be categorised as Minor and Major incidents.

Minor Incident:

When the notification is relating to, for example, a Word Macro Virus, which has only infected one PC, and the action performed on the virus is 'cured' or 'deleted'.

Major Incident:

If it's a virus that has the potential to spread to other PC's on the Trust's network, procedures should be followed to prevent this from happening:

- Helpdesk to contact user, and instruct them to shut down their PC.
- An IT Officer to get to the PC as soon as possible, and either run the virus removal software on the PC or, if necessary, run a virus killer program written specifically for the virus.
- The IT Officer should then check disks that may be infected; i.e. disks that have been used since the PC became infected.
- Helpdesk to send an e-mail to the whole Trust, with a general warning about the latest virus attack. Emphasising the instruction for users NOT to open e-mails with the virus attachment.
- In the event of a worm virus being transferred through the Trust's network, the e-mail system must be taken off-line. The mailserver to be virus scanned twice, and when clean, put system back on-line.

Reporting

Internal Reporting of Incidents:

Both the IT Manager, and the IT Security Team, should be informed if there is a minor or major virus incident. The incident should be logged by the IT Security Team in the 'Virus Incidents Log Book'. For example, what the incident was, and what action was taken. The IM&T Manager should only be informed if there's a major incident.

External Reporting of Incidents:

Any incident should be reported to the Risk management team who will forward the incident to the SHA

.

Prevention

Virus Incidents can be reduced, by following some basic investigative and preventative measures:

Source of the Virus:

The source of the virus can be pinpointed if it comes into the Trust through e-mail. The originator of the virus will be contacted, regardless of whether they are employed

by the Trust and on the Trust's Network, or if they are external to our organisation. It can be more difficult to locate the originator of a virus that comes into the Trust via a floppy disk or a CD, but it can be done. It should be the responsibility of the Network Manager, and the Security Team, to locate where the Virus' first point of contact with the Trust was.

Use Available Resources:

It is important to protect Trust PC's as much as possible, through knowledge and resources:

- Ensure that the latest virus checker signature is downloaded daily, and is being distributed Trust wide.
- PC Support Officers to ensure that older PC's have virus checker installed, and can update signature.
- All new Trust PC's are imaged. They already have the virus checker installed, and are setup to update daily.
- Check the NHSIA web site for the latest virus alert

**ATHE NEWCASTLE UPON TYNE HOSPITALS NHS FOUNDATION TRUST
IMPACT ASSESSMENT – SCREENING FORM A**

This form must be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

Policy Title:	Incident reporting policy	Policy Author:	Richard Oliver
		Yes/No?	You must provide evidence to support your response:
1.	Does the policy/guidance affect one group less or more favourably than another on the basis of:		Minor changes in layout and named officers.
	• Race	No	
	• Ethnic origins (including gypsies and travellers)	No	
	• Nationality	No	
	• Gender	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation including lesbian, gay and bisexual people	No	
	• Age	No	
	• Disability – learning difficulties, physical disability, sensory impairment and mental health problems.	No	
2.	Is there any evidence that some groups are affected differently?	No	
3.	If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?		
4(a).	Is the impact of the policy/guidance likely to be negative? <i>(If “yes”, please answer sections 4(b) to 4(d)).</i>		
4(b).	If so can the impact be avoided?		
4(c).	What alternatives are there to achieving the policy/guidance without the impact?		
4(d)	Can we reduce the impact by taking different action?		

Comments: Minor changes to existing policy, Name of security officers and telephone numbers. Layout of policy brought in line.	Action Plan due (or Not Applicable):
--	---

Name and Designation of Person responsible for completion of this form: Richard Oliver Head of Information Security & Governance..... Date:.....04/09/10.....

Names & Designations of those involved in the impact assessment screening process:..... Andy Jardine Director of IT.....

(If any reader of this procedural document identifies a potential discriminatory impact that has not been identified on this form, please refer to the Policy Author identified above, together with any suggestions for the actions required to avoid/reduce this impact.)

For advice on answering the above questions please contact Helen Lamont, Director of Nursing, or, Christine Holland, Senior HR Manager. On completion this form must be forwarded electronically to Steven Stoker, Clinical Effectiveness Manager, (Ext. 24963) steven.stoker@nuth.nhs.uk together with the procedural document. If you have identified a potential discriminatory impact of this procedural document, please ensure that you arrange for a full consultation, with relevant stakeholders, to complete a Full Impact Assessment (Form B) and to develop an Action Plan to avoid/reduce this impact; both Form B and the Action Plan should also be sent electronically to Steven Stoker within six weeks of the completion of this form.