Walton Centre

Incident Reporting

Document History

Date	Version	Author	Changes
01/10/2004	1.0	A Cobain L Wyatt	
06/01/2005	1.1	L Wyatt	Update of legislation
01/04/2005	1.2	L Wyatt	Update to version control

Table of Contents

Section	Contents
1	Introduction
2	Responsibilities Within This Standard
3	Incident Management
4	Incident Reporting
5	Compliance

APPENDICES

1. Introduction

Information and information systems are important assets and it is essential to take all the necessary steps to ensure that they are at all times protected, available and accurate to support the operation and continued success of The Walton Centre.

The Trust acknowledges that we must demonstrate to our stakeholders our commitment to, and delivery of, effective information governance.

The aim of The Walton Centre's Security Policy, Standards and Guidelines is to maintain the quality, confidentiality, and availability of information stored, processed and communicated by and within The Walton Centre. These policies, standards, guidelines are used as part of the information security management system (ISMS) within The Walton Centre.

The Walton Centre places great reliance upon the robust application of the policies and standards that make up the ISMS and has, therefore, developed processes to self assess compliance and for independent review, by its internal auditors.

This standard applies to all staff, whether permanent, part-time or temporary with responsibilities defined below.

2. Responsibilities Within This Standard

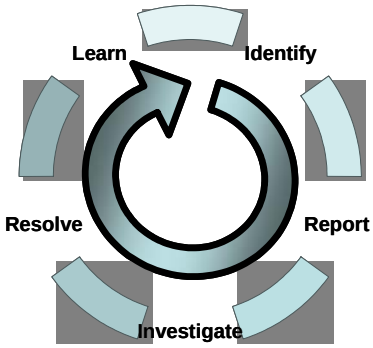
All employees using IT equipment, the internet or e-mail have responsibilities with regard to this standard. Particular responsibilities within the standard are defined as:-

Review and Maintenance	Information Security Officer
Approval	Information Security and Governance Group
Local adoption	Line Managers (in scope)
Compliance	All staff and contractor (in scope)
Monitoring	Information Security Officer Information Security Auditor

3. Incident Management

3.1 Context

This standard covers two separate but closely related areas: incident reporting, and incident response. Incident management is a cyclical process that requires identification/reporting of incidents, investigations and resolution and learning to reduce the risk of recurrence.



3.2 Definitions

An incident can generally be described as an event which has or could lead to a breach of policy, security, confidentiality or legislation or regulation. It also embraces the day to day problems encountered by users such as faults etc. In summary these can be described thus:-

- **Operational** Day to day operational issues which are traditionally channeled through Help Desks such as user queries etc.
- **Policy** Represents any failure to comply with the Trust's Information Governance Policy and its supporting standards.
- **Security** These generally fall into one of three areas viz:-

  Confidentiality – that is, incidents related to accidental or intentional leakage of confidential data, passwords and the like to unauthorized persons and organizations.

  Integrity – that is, accidental or intentional damage to or inaccuracies in data.

  Availability – that is, accidental or deliberate, disruption or absence of information and information services i.e. systems being "down", pc's not functioning correctly etc

Legislation & regulation

There is a range of legislation relating to the handling and use of information to which The Walton Centre is subject. Primarily, but not exclusively, these include:-

- Data Protection Act 1998
- Human Rights Act 1998
- Access to Health Records Act 1990
- Freedom of Information Act 2000
- Health and Social Care Act 2001
- Crime and Disorder Act 1998
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000
- Electronic Communications Act 2000
- Civil Evidence Act 1995
- Copyright, Designs and Patents Act 1988
- Health & Safety at Work Act 1974
- Defamation act of 1996
- Obscene publications act 1959

The requirements of these acts are summarised within Appendix A.

The Walton Centre is also subject to NHS guidance e.g the Information Governance requirements.

Incident reporting can be sub-divided into two main areas of interest:

- Reporting incidents as part of the incident management process.
- Reporting incidents as part of an ongoing process of collecting data on incidents in order to extract statistical data and trend analysis, with a view to improving the Trusts security and governance processes.

Incident response relates to the manner in which the organisation investigates and resolves incidents in accordance with this standard and its statutory and other obligations. The processes for resolution are described within:-

- **SS12b** - Incident Response (Legal & Forensics)
- **SS12c** - Incident Response (Operational)

4. Incident Reporting

4.1 Reporting Channels

4.1.1 Reporting Options

Individuals may become aware of actual or potential “incidents” through a variety of means, e.g. a system malfunction, a system being down or general observations regarding working practices. In all instances, it is the individual’s responsibility to ensure such incidents are reported through the appropriate channels and that such reports are directed to the most appropriate officers for investigation and resolution.

In order that the incident may be properly recorded and responded to it is essential that they are, in the first instance reported to the IT Help Desk. It is acknowledged, however, that there may be instances in which an individual may wish to make an anonymous report and as such, The Walton Centre also has in place arrangements for “whistle blowing”. These processes are described in the sections below.

4.1.2 Helpdesk Reporting

It is envisaged that the majority of incidents will be reported via the IT Help Desk in the first instance. Where an individual becomes aware of an incident or of the potential for an incident to occur they should report it to the IT Helpdesk on Insert detail.

The Help Desk staff will log all calls and will require details including:-

- End User
- Asset (computer the end user is working on if there is a specific fault with the computer)
- Asset location
- Site
- Request Type
- Problem Summary

- Problem Description
- Priority
- Owned By
- Assigned to
- Assign to Group
- Solution Base
- Solution Description

Where incidents are classified as being of an operational nature, i.e. user queries and minor faults, these will be dealt with by IT staff in accordance with:-

- **SS12c** - Incident Response (Operational)

If the "incident" is deemed to be a breach of policy, security or legislation this will be reported immediately, by the Help Desk staff, to the Head of IT and will be dealt with in accordance with:-

- **SS12b** - Incident Response (Legal & Forensics)

4.3 Line Management

Where there has been a suspected breach of policy, security or legislation employees have a right and duty to raise such matters with the Trust who, in turn, has a duty to ensure employees can easily express their concerns through all managerial levels and that employee concerns are dealt with thoroughly and fairly.

Staff are encouraged to report concerns, other than those which are operational and reported directly to the helpdesk, to their line manager who will initiate appropriate investigation.

4.3 Whistle blowing

It is acknowledged that in some instances an individual may have concerns regarding an incident or potential incident which he or she does not feel comfortable reporting to their line manager.

The Trust recognises that staff may want to raise a concern in confidence under this procedure and will not disclose an identity without consent. It should be noted, however, that if a concern is raised anonymously, it is much more difficult for the Trust to be able to investigate the matter.

Issues raised in this manner will be addressed in accordance with the Trust's "Whistleblowing Policy" [Outside of the scope of the ISMS].

5. Compliance

5.1 Responsibility

It is the responsibility of all users to ensure that they have read, understood and abide by this standard.

5.2 Review and Monitoring

The Walton Centre has in place routines to regularly audit compliance with this and other standards.

APPENDIX A

OVERVIEW OF APPLICABLE LEGISLATION

A.1 Data Protection Act 1998

All information and data which can identify a person, held in any format (visual / verbal / paper / computer / microfilm / etc.) is safeguarded by the Data Protection Act 1998, which is influenced by eight principles:

- **FIRST PRINCIPLE** Personal data shall be processed fairly and lawfully.
- **SECOND PRINCIPLE** Personal data shall be obtained only for one or more specified and lawful purpose(s), and shall not be further processed in any manner incompatible with that purpose or those purposes.
- **THIRD PRINCIPLE** Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- **FOURTH PRINCIPLE** Personal data shall be accurate and, where necessary, kept up to date.
- **FIFTH PRINCIPLE** Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- **SIXTH PRINCIPLE** Personal data shall be processed in accordance with the rights of data subjects under this Act.
- **SEVENTH PRINCIPLE** Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- **EIGHTH PRINCIPLE** Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

All NHS development in the area of security and confidentiality will need to be carried out within the provisions of the Act. This is the relevant enabling legislation to implement the EU Data Protection Directive and which has had effect in the UK from 24 October 1998.

For the NHS this means:

- Vigilance over privacy.
- Transparency over process.
- Winning and keeping patients trust.
- Addressing the privacy as well as the technological challenges of modernisation.

This can be achieved by:

- Clarity about rules and standards.
- Transparency as a means of building trust.
- Better record keeping.
- Clear legal basis for activities.
- Active use of privacy enhancing technologies (PETS).

If the NHS is to make the best use of technology to deliver improved 'joined up' services, then understanding, respecting and promoting rights must be seen as objectives.

A.2 Human Rights Act 1998

The Human Rights Act 1998 (HRA) came into force in the United Kingdom on 2 October 2000. It incorporates the rights and freedoms set out in the European Convention on Human Rights. The English Courts must take into account decisions of the European Court of Human Rights. The HRA applies to 'public authorites' who may not do anything or fail to do something which contravenes the HRA. Public authorities may sometimes have a positive duty to protect the rights of individuals as well as a duty simply not to interfere with those rights. An individual can use the HRA as a shield in any claim by a public authority, even if the act or omission of the public authority was prior to 2 October 2000. Victims can be awarded damages for a breach of their Convention rights.

Private individuals or bodies can not be taken to Court under the HRA, only public authorities. However, it may come to have an indirect effect here too.

The HRA creates a new obligation on public authorites to act compatibly with the Convention, as well as the existing legislation under which they operate. There are enormous social, economic and health benefits flowing from increasingly efficient methods of recording patient information. However the potential use of information stored in electronic health records raises serious concerns about unauthorised or unfair access about patient privacy.

The Convention rights are set out in the HRA as 'Articles'. Not all rights are absolute and unconditional. A public authority would have a defence if another Act of Parliament required them to act in a way which breached an individual's rights. A number of principles underpin the interpretation of the Convention rights:

Legality – all restrictions must be lawful.

Proportionality – there must be a fair balance. The public authority must give reasons which are 'relevant and sufficient'. Are there less restrictive alternatives? Has the public authority acted with procedural fairness and are there adequate safeguards in place?

Legitimate Aim – the restrictions in the Convention rights set out the aims to be achieved which include national security; public safety; the protection of health or morals; the prevention of disorder or crime; the protection of the rights of others.

Necessity – the restriction must be necessary in a democratic society. Is there a pressing social need for some restriction? If so, does the actual restriction address that need? Is the restriction proportionate? Are the reasons 'relevant and sufficient'?

Access to and release of information are subjects that frequently concern health professionals. The NHS as a public body must always ensure that it does not act in a way that is incompatible with a Convention right.

The relevant Articles here are:

- **Article 6** – Right to a fair hearing – patients should be made aware of procedures which enable them to seek all relevant and appropriate information.
- **Article 8** – Right to respect for family and private life – unauthorised disclosure of patient records is a breach of this Article, although there are cases where exceptions are likely to apply.
- **Article 14** – Prohibition of discrimination – it would be in contravention of the HRA not to allow a person access to their health records on the grounds of their sex, race, colour, membership of a political party, etc. Also, information provided must be in a form accessible to those suffering from sensory impairments or those who can not speak English or may have other difficulties in understanding the information.

A.3 Access to Health Records Act 1990

The Access to Health Records Act 1990 formerly gave individuals a right of access to manual health records, i.e. non-automated records. However, this Act has now been repealed by the Data Protection Act 1998, except for the sections dealing with access to the records of deceased patients.

A.4 Freedom of Information Act 2000

The Freedom of Information Act 2000 became law on 30 November 2000 and will be enforced by the Information Commissioner, a new post that combines Freedom of Information and Data Protection. Both the Freedom of Information Act and the Data Protection Act relate to information handling and this dual role will allow the Information Commissioner to provide an integrated and coherent approach.

The Act gives a general right of access to information of all sorts held by public authorities and those providing services for them, sets out exemptions from that right and places a number of obligations on public authorities.

Implementation of the Act will be gradual, it being fully implemented by January 2005. Only public authorities are covered by the Act, which include Central Government Departments, local Government, local authorities, NHS bodies, the Police, Crown Prosecution Service, Serious Fraud Office, Armed Forces, and education establishments.

The requirement for each public authority to adopt a 'publication scheme' will come into force first, with NHS organisations by October 2003. The individual right of access to information will come into force for all public authorities in January 2005.

Freedom of Information (FOI) will extend 'subject access rights' (under the Data Protection Act 1998) to allow access to all the types of information public bodies hold, whether personal or non-personal. However, some of the information requested need not be provided if one of the exemptions in the Act applies.

Anyone will be able to make a request for information, although the request must be in permanent form. The Act gives applicants two related rights:

- The right to be told whether the information exists.
- The right to receive the information.

Applicants will not be able to exercise their right of access until January 2005. However, applicants will then still be able to request information recorded before the Act was passed i.e. information produced before 30 November 2000, if such information is still being retained in line with the suggested minimum retention periods as set out in Health Service Circular 1999 / 053 – For the Record.

There are 23 exemptions in the Act e.g. information need not be released if it would prejudice national security, or law enforcement. Some exemptions apply to a whole category of information e.g. information relating to investigations and proceedings conducted by public authorities, court records, and trade secrets. Other exemptions are subject to a prejudice test e.g. where disclosure would or would be likely to prejudice the interests of the United Kingdom abroad, or the prevention or detection of crime.

A.5 Health and Social Care Act 2001

Section 60 of the Health and Social Care Act 2001 enables the Secretary of State to support and regulate the use of confidential patient information in the interest of patients or the wider public good. Parliament agreed to the creation of this power to ensure that patient identifiable information currently needed to support essential NHS activity can be used, without the consent that should normally be obtained**, *where there is no reasonably practicable alternative*.**

Regulations made under Section 60 can provide a basis in law for patient identifiable information to be disclosed to specified bodies, (e.g. cancer registries), for specific purposes. This type of '**specific support'** is required if the intended purposes for obtaining the information are controversial or complex and need detailed description within the regulations. The approval of Parliament, advised by the independent statutory Patient Information Advisory Group (PIAG), is required before such regulations may be brought into force.

Parliament has also agreed to the establishment of '**class support**' that will provide a lawful basis for using and disclosing patient identifiable information to support relatively uncontroversial processing, for limited and defined purposes, without the need for dedicated Parliamentary consideration. The approval of the Secretary of State, advised where appropriate by PIAG, is required in these circumstances.

Section 60 requires an annual review of the regulations. The Secretary of State, supported by PIAG, will keep under review the need for support and aim to revoke it as soon as it is practicable. Support under Section 60 is intended as a transitory measure. That said, there might be a small number of uses for which informed consent or anonymisation will never be practicable. Through transparent and robust annual review, Section 60 will be used to determine whether or not this is the case. In these instances, specific and permanent legislation may be the solution.

Section 60 support is not unconditional. A number of requirements impact upon those who receive support, with the twin goals of ensuring that there are adequate safeguards for patients and that options for improving consent practice and/or introducing anonymisation techniques are actively pursued.

A.6 Crime and Disorder Act 1998

The Crime and Disorder Act 1998 requires the police and local authorities to work together, in partnership with other agencies, to develop and implement a strategy for reducing crime and disorder, with the goal of actually delivering safer communities. The Act places new obligations on those involved to co-operate in the development and implementation of a strategy for tackling crime and disorder in their area. This will require substantial changes in the working practices of all these organisations, thinking in new and different ways about their own internal priorities and their relationship both with other agencies and with the wider community.

The Act requires local Councils and the Police to:

- conduct and publish an audit of local crime and disorder problems.
- consult locally on the basis of the audit.
- set and publish objectives and targets for the reduction of crime and disorder.
- monitor progress.
- repeat the process every three years.

The Act is intended to facilitate the exchange of information between agencies for the purpose of the Act. Partners will have to overcome the challenges presented by non-coterminous agency boundaries and non-compatible data.

The NHS has a key role in any crime and reduction strategy, because it is a universal service, which reaches all sectors of the population. This allows the health service to be involved in the direction of some forms of crime (such as domestic violence) and consequently the prevention of repeat offending, as well as in behaviour modification strategies, particularly for young people.

Very few of the partners have coterminous boundaries and the agencies involved are not responsible for precisely the same geographical area as their partners. The focus of the audit and strategy is the local authority area. To ease inter-agency co-operation all partners should tailor their information collection practices so that different sets of data can more readily be compared using different combinations of the same 'building blocks'.

Before disclosing information consider if information needs to be disclosed in a form which allows individuals to be personally identified. The best way of ensuring that disclosure is properly handled is to operate within clear 'Information Sharing Protocols', which address:

- the purpose of the information sharing arrangement.
- whether necessary to share personal information.
- whether the parties have the power to disclose personal information.
- how much personal information should be shared.
- whether the consent of the individual should be sought.
- what if consent is not sought, or is sought but withheld.
- how does the non-disclosure exemption apply.
- how to ensure compliance with other Data Protection Act 1998 principles.

A.7 Computer Misuse Act 1990

Under the Computer Misuse Act 1990 computer hacking or introduction of viruses are criminal offences. The Act covers three types of offence:

- Unauthorised access to computer material (program and / or data).
- Unauthorised access to computer systems with intent to commit or facilitate a serious crime.
- Unauthorised modification of computer material.

A.8 Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 is commonly known as RIPA.

The Act updates the law on interception of communication, taking into account the technical change such as growth of the Internet.

The Act puts other intrusive investigative techniques on a Statutory footing, thus providing power to aid in combat of threats posed by the rise of criminal use of strong encryption and ensures independent judicial oversight of the powers in the Act. There is a clash with this Act and the Human Rights Act 1998.

Consideration of this Act should be given by organisations with a need to incorporating it into e-mail and telephone procedures.

A.9 Electronic Communications Act 2000

This Act has three sections, which will have relevance to electronic records in the NHS.

Cryptography and service providers, together with electronic signatures fall under the Act.

A.10 Civil Evidence Act 1995

There are Civil Procedures 2000 as part of The Civil Evidence Act 1995.

The Act is in two parts:

Part I - Includes the reliability of computer evidence against the evidence in business and paper documentation held.

Part II - Information Management Method, and Good Practice for Information Management to assist with litigation.

A.11 Copyright, Designs and Patents Act 1988

The Copyright, Designs and Patents Act 1988 (and amending legislation) is reproduced under the terms of Crown Copyright Policy Guidance issued by HMSO. This Act is to restate the law of copyright, with amendments, and includes the following for example to:

- confer a design right in original design
- amend the Registered Designs Act 1949
- make provision with respect to patent agents and trade mark agents
- amend the law of patents
- make provision with respect to devices designed to circumvent copy-protection of works in electronic form
- make fresh provision penalising the fraudulent reception of transmissions
- make the fraudulent application or use of a trade mark an offence

A.12 Health & Safety at Work Act 1974

There is a section in this Act on visual display units (VDUs) that must be adhered to, which are the Display Screen (VDU) Regulations.

This covers six main obligations by the employer to employees who use VDU equipment.

The Health and Safety (Display Screen Equipment) Regulations 1992 became part of the Act in January 1993.

A.13 Defamation act of 1996

Provides a defence to persons who are not authors, editors or commercial publishers of the statement if they took reasonable care in relation to its publication and they did not know and had no reason to believe that what they did caused or contributed to the publication of a defamatory statement. This is intended to cover printers, distributors, on-line service providers and live broadcasters

A.14 Obscene publications act 1959

The "Obscene Publications Act 1959 and 1964" states that an article shall be deemed to be obscene if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

It is an offence to publish an obscene article or to have an obscene article in ownership, possession or control with a view to publishing it or, where the data is stored electronically, to transmit that data.

The "Telecommunications Act 1984" makes it an offence to send 'by means of a public telecommunications system, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character'. The maximum prison term is six months.