Maidstone and Tunbridge Wells NHS Trust

Ref: FOI/CAD/ID 3339

**Please reply to:**
FOI Administrator
Trust Management
Service Centre
Maidstone Hospital
Hermitage Lane
Maidstone
Kent
ME16 9QQ
Email: mtw-tr.foiadmin@nhs.net

23 May 2016

**Freedom of Information Act 2000**

I am writing in response to your request for information made under the Freedom of Information Act 2000 in relation to breaches of the Data Protection Act.

*1a.Approximately how many members of staff do you have?*
*1b.Approximately how many contractors have routine access to your information?*

*2a.Do you have an information security incident/event reporting policy/guidance/management document(s) that includes categorisation/classification of such incidents?*
*2b.Can you provide me with the information or document(s) referred to in 2a? (This can be an email attachment of the document(s), a link to the document(s) on your publicly facing web site or a 'cut and paste' of the relevant section of these document(s))*

*3a.Do you know how many data protection incidents your organisation has had since April 2011? (Incidents reported to the Information Commissioners Office (ICO) as a Data Protection Act (DPA) breach)*
*Answer: Yes, No, Only since (date):*
*3b.How many breaches occurred for each Financial Year the figures are available for?*
*Answer FY11-12: FY12-13: FY13-14: FY14-15:*

*4a.Do you know how many other information security incidents your organisation has had since April 2011? (A breach resulting in the loss of organisational information other than an incident reported to the ICO, eg compromise of sensitive contracts or encryption by malware. )*
*Answer: Yes, No, Only since (date):*
*4b.How many incidents occurred for each Financial Year the figures are available for?*
*Answer FY11-12: FY12-13: FY13-14: FY14-15:*

*5a.Do you know how many information security events/anomaly your organisation has had since April 2011? (Events where information loss did not occur but resources were assigned to investigate or recover, eg nuisance malware or locating misfiled documents.)*
*Answer: Yes, No, Only since (date):*
*5b.How many events occurred for each Financial Year the figures are available for?*
*Answer FY11-12: FY12-13: FY13-14: FY14-15:*

*6a.Do you know how many information security near misses your organisation has had since April 2011? (Problems reported to the information security teams that indicate a possible technical, administrative or procedural issue.)*
*Answer: Yes, No, Only since (date):*
*6b.How many near-misses occurred for each Financial Year the figures are available for?*
*Answer FY11-12: FY12-13: FY13-14: FY14-15:*

1a. 5,902
1b. The Trust has estimated that it will cost more than the appropriate limit to consider this part of your request. The appropriate limit is specified in regulations and represents the estimated cost of one person spending 3½ working days in determining whether the Trust holds the information, locating, retrieving and extracting the information. Under Section 12 of the Freedom of Information Act 2000 the Trust is not obliged to comply with this part of your request and we will not be processing this part of your request further.

2a. Yes
2b. Please see the attached policy.

3a. This information is available in the Trust Report and Accounts which can be found on our website using the following link: http://www.mtw.nhs.uk/about-us/publications/
3b. This information is available in the Trust Report and Accounts which can be found on our website using the following link: http://www.mtw.nhs.uk/about-us/publications/

4a. This information is available in the Trust Report and Accounts which can be found on our website using the following link: http://www.mtw.nhs.uk/about-us/publications/
4b. This information is available in the Trust Report and Accounts which can be found on our website using the following link: http://www.mtw.nhs.uk/about-us/publications/

5a. This information is available in the Trust Report and Accounts which can be found on our website using the following link: http://www.mtw.nhs.uk/about-us/publications/
5b. This information is available in the Trust Report and Accounts which can be found on our website using the following link: http://www.mtw.nhs.uk/about-us/publications/

6a. This information is available in the Trust Report and Accounts which can be found on our website using the following link: http://www.mtw.nhs.uk/about-us/publications/
6b. This information is available in the Trust Report and Accounts which can be found on our website using the following link: http://www.mtw.nhs.uk/about-us/publications/

MAIDSTONE AND TUNBRIDGE WELLS NHS TRUST

Information Security Incident Reporting

Requested/
Required by: Information Governance Steering Committee
Overarching policy /
procedure: Incident Management Policy and Procedure [RWF-OPPPCS-NC-CG22]
Main author: Director of ICT
Other contributors: Walton Centre for Neurology and Neurosurgery NHS Trust
Document lead: Director of ICT
Contact: ext. 22048
Directorate: Corporate
Specialty: Trust Management
Supersedes: Information Security Incident Reporting Policy and Procedure (Version 1.0: September 2010)
Approved by: See overarching policy / procedure
Ratified by: See overarching policy / procedure
Review date: March 2016

IG Toolkit Ref: 8-302
MTW ICT Asset Ref TBC

Disclaimer: Printed copies of this document may not be the most recent version.
The master copy is held on Q-Pulse Document Management System
This copy – REV2.0

Document history

| | |
|---|---|
| Requirement for document: | • This document is required to provide assurance that breaches in information security are reported and managed appropriately.<br>• The document is required to support business processes and meets the requirements of the NHS Information Governance Toolkit. |
| Cross references: | 1. NHS Business Continuity Planning Manual<br>2. CfH Good Practice in Mobile Computing<br>3. Data Protection Act 1998<br>4. Human Rights Act 1998<br>5. Access to Health Records Act 1990 |

| | |
|---|---|
| | 6. Freedom of Information Act 2000<br>7. Health and Social Care Act 2001<br>8. Crime and Disorder Act 1998<br>9. Computer Misuse Act 1990<br>10. Regulation of Investigatory Powers Act 2000<br>11. Electronic Communications Act 2000<br>12. Civil Evidence Act 1995<br>13. Copyright, Designs and Patents Act 1988<br>14. Health & Safety at Work Act 1974<br>15. Defamation Act 1996<br>16. Obscene Publications Act 1959 |
| Associated documents: | 17. Maidstone and Tunbridge Wells NHS Trust. *Policy for the Use of Removable ICT Media* [RWF-OPPCS-NC-TM15]<br>18. Maidstone and Tunbridge Wells NHS Trust. *Safe Haven - Safe Transfer of Person Identifiable Information, Policy and Procedure for the* [RWF-OPPCS-NC-TM16]<br>19. Maidstone and Tunbridge Wells NHS Trust. *Remote Access Policy and Procedures*<br>20. Maidstone and Tunbridge Wells NHS Trust. *Records Retention Policy* [RWF-OPPCS-NC-TM17]<br>21. Maidstone and Tunbridge Wells NHS Trust. *Forensic Readiness Policy*<br>22. Maidstone and Tunbridge Wells NHS Trust. *Incident Management Policy and Procedure* [RWF-OPPPCS-NC-CG22]<br>23. Maidstone and Tunbridge Wells NHS Trust. *Whistle Blowing Policy and Procedure* [RWF-OPPPCS-NC-WF33]<br>24. Maidstone and Tunbridge Wells NHS Trust. *Serious Incidents Requiring investigation (SIRI) Policy and Procedure* [RWF-OPPPCS-NC-CG23]<br>25. Maidstone and Tunbridge Wells NHS Trust. *Display Screen Equipment Policy and Procedure* [RWF-OPPPCS-NC-CG17]<br>26. Maidstone and Tunbridge Wells NHS Trust. *Staff Leaflet - Keeping Information Safe a summary of what you need to know* |

| Version control: | | |
|---|---|---|
| Issue: | Description of changes: | Date: |
| 1.0 | First iteration | September 2010 |
| 1.1 | Reviewed. No longer a policy and procedure but an appendix of the “Incident Management Policy and Procedure” | November 2013 |
| 2.0 | Appendix to Incident Management Policy and Procedure which was reviewed and approved by Health and Safety Committee, 24th February 2014 and ratified by: Quality and Safety Committee, 5th March | March 2014 |

| | | |
|---|---|---|
| | 2014 | |

Information Security Incident Reporting Procedure

Contents Page



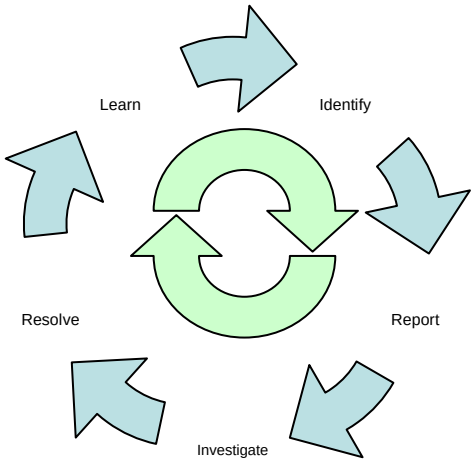
Appendices



## 1.0 Introduction and scope

Information and information systems are important assets and it is essential the Trust takes all necessary steps to ensure that they are at all times protected, available and accurate.

Incident management is a cyclical process that requires identification / reporting of incidents, investigations and resolution and learning to reduce the risk of recurrence.




This document sets out guidance to staff on the type of incidents which are classified as information security and confidentiality incidents, and to whom they should be

reported. This document should be used in combination with the Trust Incident Management Policy and Procedure and the Serious Incident Requiring Investigation (SIRI) Policy and Procedure. It is intended to supplement these policies rather than replace them.

The document applies to all staff in all disciplines discovering or otherwise observing an information security or confidentiality incident, in relation to patient and staff information.

## 2.0 Definitions

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

Operational Day to day operational issues which are traditionally channelled through Help Desks such as user queries, etc.

Policy Represents any failure to comply with the Trust's Information Governance policies and their supporting procedures

Security These generally fall into one of three areas:

Confidentiality – these are incidents related to accidental or intentional leakage of confidential data or user access rights (passwords) to unauthorised persons and organisations.

Integrity – accidental or intentional damage to or inaccuracies in data;

Availability – accidental or deliberate disruption or absence of information and information services i.e., systems being 'down', PCs not functioning correctly, etc.

An information security/confidentiality incident is defined as any event that has resulted or could result in:

- The disclosure of confidential information to any unauthorised individual.
- The integrity of the system or data being put at risk.
- The availability of the system or information being put at risk.

In all cases 'data' refers to both manual and computer data, and thus all record keeping and filing incidents come within the remit of this document.

Legislation and regulation – the Maidstone & Tunbridge Wells NHS Trust is subject to a wide range of legislation relating to the handling and use of information.

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 1996
- Obscene Publications Act 1959

Further information on supporting legislation is at Appendix 4.

## 3.0 Duties (roles and responsibilities)

Roles and responsibilities as defined in the Information Governance Management Framework are set out in Appendix 5.

4.0 Training / competency requirements

All staff are trained to report incidents as part of the corporate and local induction programmes. An e-learning package has been developed to train all staff in e-reporting and is available 24 hours a day through the internet. E-reporting was rolled out throughout the Trust during 2010/2011. During the summer of 2010 a new electronic investigation tool was rolled out to senior managers to assist in information gathering as part of SIRI investigations.

In addition the Risk Team will co-ordinate specific training for incident investigators. They will be trained in Root Cause Analysis tools. The Risk and Patient Safety Team will co-ordinate training for all Trust managers and directors to enable them to perform their duties under this document. The Risk Manager will also deliver Risk Management Training to the Board.

5.0 Types of information security / confidentiality incidents

There are basically four types of incident which relate to information security and confidentiality.

5.1 A security incident

Examples of this type of incident include:

- Theft of equipment holding confidential patient or staff information
- Computer equipment (processors, laptops, disks, CDROMs)
- Dicta-phones, tapes
- Malicious damage to such equipment
- Loss of such equipment
- Unauthorised access to a building or areas containing unsecured confidential information
- Car theft / break-ins where staff are carrying patient records

*Reporting procedure*

*Immediate actions*

In the event of a theft of or damage to computer equipment, staff must complete an e-reporting incident form (DIF1) (see reference 22) and report the incident to the following:

1. The Trust Security Manager – Who will instigate a police call-out, to ensure that the crime is properly recorded and to enable forensic evidence to be obtained. (It is important that at this stage staff should make every attempt not to use the area where the crime has been committed to avoid contamination of any evidence).

   The Trust Security Manager will inform ICT Manager of the theft and obtain relevant details relating to equipment identification and cost etc.
2. Line Manager - at the earliest opportunity.
3. Head of Information Governance (ext. 26418) – if patient or staff information is believed to have been lost.
4. The incident may be an SIRI and require reporting to the SHA/PCT (see reference 24). If a possible SIRI the Head of Quality and Governance must be informed.

*Follow up actions*

1. On arrival, the Police Officer/s will be escorted to the scene of the crime by a Security Officer. The Police Officer/s will liaise with the staff member reporting the crime, take a statement to identify the equipment stolen and approximate costs.

2. The Security Manager will visit the crime scene at the earliest opportunity, to identify the cause of the incident and to instigate procedures to ensure that preventative measures are implemented to minimise the risk of reoccurrence.
3. The incident will be recorded onto the Security Department incident database. These details will be used to produce a crime pattern analysis and identify problem areas.
4. The Security Manager will compile a comprehensive report on the incident, including recommendations to be instigated as soon as possible, in order to protect Trust assets from further crime.
5. If an SIRI the SHA/PCT must be kept informed and the incident discussed and signed off by the SIRI panel (see reference 24).

Copies of the report will be sent to the following:

- Director of Finance
- Internal Audit
- Director of ICT
- Head of Information Governance
- Head of Quality and Governance (SIRI panel).
- Director of Estates and Facilities
- Head of Department

Unauthorised access to a building or areas containing unsecured confidential information and Car theft / break-ins where staff are carrying patient records. If information is missing the reporting arrangements are the same as for thefts of computer equipment above. The Security department may not call the police to these incidents. If information is not missing (i.e. a near miss has occurred).

Staff must complete an e-reporting incident form (DIF1) (see reference 22) and report the incident to the following:

1. Line manager, at the earliest opportunity, who will:

- Undertake an immediate investigation
- Notify and liaise with the Head of Information Governance re the recommendations arising

2. The incident may be a SIRI and require reporting to the SHA/PCT (see reference 24). If a possible SIRI the Head of Quality and Governance must be informed.

5.2 An information and communications technology (ICT) incident

Examples of this type of incident include:

- Password sharing, not logging off terminals
- Unauthorised electronic access (hacking) and viruses.
- Non compliance to Trust internet and email policies
- Malicious damage to information held on computer
- Unauthorised software loaded and used, either purchased privately, or downloaded from the internet
- Inappropriate location of terminals allowing inappropriate access to patient information

*Immediate actions*

In the event of any of these incidents occurring, staff must complete an e-reporting incident form (DIF1) (see reference 22) and report the incident to the following:

1. Line manager and ICT Manager who will:

- Undertake immediate investigation and determination whether an IT security breach has occurred.
- Liaise with the Head of Information Governance where patient/staff records issues are involved.

2. The incident may be an SIRI and require reporting to the SHA/PCT (see reference 24). If a possible SIRI the Head of Quality and Governance must be informed.

*Follow up actions*

The Information Asset Owner will compile a comprehensive report on the incident, including recommendations to be instigated as soon as possible. Copies of the report will be sent to the following:

- Head of Information Governance / Caldicott Guardian
- Head of Quality and Governance (SIRI panel)
- Head of Department
- Director of Finance if there are any financial implications for the Acute Trust
- Workforce Director to determine whether any disciplinary action is necessary

In the event of a near miss, staff must complete an e-reporting incident form (DIF1) and report the incident to the following:

1. Line manager, at the earliest opportunity, who will

- Undertake immediate investigation
- Notify and liaise with the ICT Manager re the recommendations arising

5.3 A breach of confidentiality

Examples of this type of incident include:

- Access to patient records (electronically or physically in the case notes) by an authorised user who has no work requirement to access the records, e.g. looking at the records of relatives or staff, leaving case notes unattended in corridors or other public areas
- Unauthorised access to records away from premises (e.g. laptops and notes when travelling between clinics to home-visits etc).
- Unauthorised sharing of information with other agencies, e.g. police
- Inadequate disposal of confidential material (paper, PC hard drive, disks / tapes, etc).
- Sending a sensitive e-mail to ‘all staff’ by mistake
- Complaint by a patient or a member of the public, that confidentiality has been breached.
- Discussing patient or staff personal information with someone else in an open area where the conversation can be overheard
- Misuse of equipment such as faxes, text messages on mobiles and e-mails
- A fax being received by an incorrect recipient
- Malicious damage to information held on paper, e.g. case notes

*Immediate actions*

In the event of any of these incidents occurring, staff must complete an e-reporting incident form (DIF1) (see reference 22) and report the incident to the following:

1. Line manager, who will

- Undertake immediate investigation and action
- Liaise with Head of Information Governance with regard to follow up actions

2. The incident may be an SIRI and require reporting to the SHA/PCT (see reference 24). If a possible SIRI the Head of Quality and Governance must be informed.

*Follow up actions*

The line manager supported by the Information Asset Owner will compile a comprehensive report on the incident, including recommendations to be instigated. Copies of the report will be sent to the following:

- Caldicott Guardian
- Head of Quality and Governance (SIRI panel).
- Head of Department
- Director of Finance if there are any financial implications for the Trust
- Workforce Director to determine whether any disciplinary action is necessary

The Head of Information Governance will compile a quarterly report on the incidents and actions taken for the Health Records Committee and Caldicott Guardian

5.4 An incident concerning record keeping

Examples of this type of incident include:

- Loose documents inside case note folders rather than filed.
- Documents/photographs relating to different patients in the same case note folder.
- Merging of case notes or other records (e.g. casualty cards) of patients with the same or similar names, either manually or on computer or both.

In the event of any of these incidents occurring, staff must complete an e-reporting incident form (DIF1) (see reference 22) and report the incident to the following:

The line manager, who will:

- Undertake immediate investigation and action
- Liaise with Head of Information Governance with regard to follow up actions

The line manager, supported by the Information Asset Owner, will compile a comprehensive report on the incident, including recommendations to be instigated as soon as possible. Copies of the report will be sent to the following:

- Caldicott Guardian
- Head of Department
- Director of Finance if there are any financial implications for the Trust
- Workforce Director to determine whether any disciplinary action is necessary

The Head of Information Governance will compile a quarterly report on the incidents and actions taken for the Health Records Committee and Caldicott Guardian.

6.0 Reporting requirements for breaches in Information Governance

If in any of the incidents patient confidentiality has been or is suspected of being breeched the incident must be assessed against the Information Governance Serious Untoward Incident procedures and an appropriate report made to the SHA and to the Information Commissioner's Office if required. The assessment of the incident severity will be managed by the Head of Information Governance or the Caldicott Guardian and will be in line with the Serious Incident Requiring Investigation (SIRI) Policy and Procedure.

7.0 Forensic readiness

Information Governance staff from the Kent and Medway Health Informatics Service (HIS) may be asked to assist in any forensic analysis that may be required after an incident.

8.0 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 'Whistle Blowing Policy and Procedure' (see reference 23).

9.0 Monitoring and audit

The implementation of this document will be monitored individually and collectively by the members of the Information Governance Steering Committee. Audit of compliance is a requirement of roles of the Information Asset Owners and Administrators who must report any breaches to the SIRO, the Head of Information Governance, the Caldicott Guardian and the Director of ICT. The SIRO will report major breaches to the Trust Board.

----------oOo----------

FURTHER APPENDICES

The following appendices are published as related links to the main document /procedure on the Trust approved document management database:

| No. | Title | Unique ID |
|---|---|---|
| 1 | Overview of applicable legislation | RWF-OWP-APP730 |
| 2 | Staff roles and responsibilities | RWF-OPPM-CORP178 |

**Overview of Applicable Legislation**

**A.1 Data Protection Act 1998**

All information and data which can identify a living 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 or 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 since 24 October 1998.

Disclaimer: Printed copies of this document may not be the most recent version.
The master copy is held on Q-Pulse Document Management System
This copy – REV2.0

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 authorities' 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 to.

The HRA creates a new obligation on public authorities 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 restrictions 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 a 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 these 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

Access to Health Records Act 1990 formally gave individuals a right of access to manual health records i.e., non-automated records. However, this Act has 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 is 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 allows 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 was gradual, it was fully implemented in 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’ came into force in October 2003. The individual right of access to information came into force for all public authorities in January 2005.

The Freedom of Information Act (FOIA) extended ‘subject access rights’ (under the Data Protection Act 1998) to allow access to all 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 can 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 are 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 document Gateway Ref: 6295 – Records Management: NHS Code of Practice which superseded Health Service Circular 1999/953 – 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 requires 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 areas 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 arrangements;
- 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 (programme and/or data);
- Unauthorised access to computer systems with intent to commit or facilitate a serous 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 the Act should be given by organisations with a need to incorporating it into email and telephone procedures.

### A.9 Electronic Communications Act 2000

This Act has three sections, which 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

The Act enables the Secretary of State to pass regulations. One such is the The Health and Safety (Display Screen Equipment) Regulations 1992.

The Trust adheres to this regulation. Details can be found in the Trust's Display Screen Equipment policy and procedure.

### 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 wheat 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'.