MEDICAL IMAGING
PARTNERSHIP

Data Protection Policy

Policy Type:	*Information Governance*
Reference Number	*IG02*
Version:	*1.5*
Author:	*Scott Crawford*
Created:	*May 2011*
Review Frequency:	*Annual*
Last Review Date:	*June 2018*
Next Review Date:	*June 2021*
Responsible Committee/Person:	*Executive Committee*
Date Ratified:	*19th July 2018*

Document History

Version	Comments	Author	Date
1.0	Initial Release	Scott Crawford	May 2011
1.1	Version control, document history and table of contents added.	Phoebe Cowham	Oct 2011
1.2	Update to Committee titles	Phoebe Cowham	Aug 2012
1.3	Section 14 Equality Impact Statement added	Phoebe Cowham	April 2015
1.4	Hyperlink corrected on section 7.8	Julian Arnott	Oct 2016
1.5	GDPR, Data Protection by design and default, Recording Information Security Incidents, removal of appendices. General updates.	Richard Weston	June 2018

Table of Contents

1 OVERVIEW

Medical Imaging Partnership (MIP) has a legal obligation to comply with all appropriate legislation in respect of Data, Information and IT Security. It also has a duty to comply with guidance issued by the Department of Health, the Information Commissioner, the Healthcare Commission, other advisory groups to the NHS and guidance issued by professional bodies.

All legislation relevant to an individual's right of confidentiality and the ways in which that can be achieved and maintained are paramount to MIP. This topic relates to individuals that perform tasks entailing access to data stored within computer systems such as: patient/client administration/payment, purchasing, invoicing and treatment planning and on manual records relating to patients/clients, staff and others whose information may be held within MIP's files and systems.

Penalties could be imposed upon MIP, and/or MIP employees for non-compliance with relevant legislation and NHS guidance.

This Data Protection Policy describes how MIP meets its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the UK's implementation of the General Data Protection Regulation.

For the purposes of this Policy, other relevant legislation and appropriate guidance may be referenced.

2 PURPOSE AND AIMS OF POLICY

For the purpose of this Policy other relevant legislation and appropriate guidance may be referenced. A brief summary of the relevant legislation and guidelines is set out in the next section.

MIP will evaluate practice against this policy annually to ensure its effective implementation.

3 LEGISLATION

The legislation listed below refers to issues of security and/or confidentiality of personal identifiable information/data (see Section 5 and Appendix 2 for more detailed information).

- General Data Protection Regulation
- Access to Medical Reports Act 1988
- Data Protection Act 2018
- Crime and Disorder Act 1998
- Human Rights Act 1998
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000

4 PUBLICATIONS

The following are the main publications referring to security and/or confidentiality of personal identifiable information/data (see Section 5 and Appendix 2 for more information):

- Confidentiality: NHS Code of Practice (August 2003)
- Employee Code of Practice (Information Commissioner)
- HSC2000/009 Data Protection Act 1998: Protection and Use of Patient Information
- Records Management: NHS Code of Practice (2006)
- HSC2002/3 Implementing the Caldicott Standard into Social Care
- ISO27001 International Standard for Information Security Management
- Care Quality Commission National Minimum Standards

5 OVERVIEW OF LEGISLATION & NHS GUIDANCE

5.1 General Data Protection Regulation (GDPR)

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Under GDPR, individuals have the right to find out what information the government and other organisations store about them. As an individual these include the right to:

- be informed about how your data is being used
- access personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of your data
- data portability (allowing you to get and reuse your data for different services)
- object to how your data is processed in certain circumstances
- automated decision-making processes (without human involvement)
- profiling, for example to predict your behaviour or interests

Patients' rights under GDPR are documented in Medical Imaging Partnerships privacy notice www.medicalimaging.org.uk/priacy-notice.

5.2 Data Protection Act 2018

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

5.3 Confidentiality: NHS Code of Practice

This code provides detailed guidance for NHS bodies concerning confidentiality and a patient's consent when accessing and using their health information. It also details the required practice

which the NHS (and MIP) must follow concerning security and identifies the main legal responsibilities for an organisation and its employees (www.dh.gov.uk).

5.4 Employee Code of Practice

Guidance produced by the Information Commissioner detailing the data protection requirements that relate to staff/employee and other individual's information (http://www.ico.gov.uk/).

5.5 Caldicott Guardians & Implementing the Caldicott Standard into Social Care HSC2002/003

Provides guidelines relating to sharing of patient/client identifiable information and promotes the appointment of a senior health professional to oversee the implementation of the guidance. It also re-iterates guidance produced in 1999 for NHS Caldicott Guardians www.dh.gov.uk (search by Confidentiality).

5.6 Records Management: NHS Code of Practice

This Code, together with the supporting annexes and in conjunction with the Roadmap, identifies the specific actions, managerial responsibilities, and minimum retention periods for the effective management of all types of NHS records (i.e. both corporate and health records) from creation, as well as day-to-day use of records, and storage, maintenance and ultimate disposal procedures.

5.7 The Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. Each organisation will issue individual user's an individual user id and password which will only be known by the individual they relate to and must not be divulged/misused by other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act.

Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

5.8 ISO 27001

This is the accepted industry standard for Information Security Management. This standard has been adopted by all NHS organisations. It is also a recommended legal requirement under principle 7 of the Data Protection Act.

6 MANAGEMENT RESPONSIBILITIES

MIP's Chief Executive Officer has overall responsibility for the Data Protection Policy. The implementation of, and compliance with, this Policy is delegated to the Integrated Governance Committee.

MIP's managers are responsible for ensuring data protection practices, compliance with this policy and staff awareness of their responsibilities concerning data protection compliance.

MIP has appointed the Medical Director as the 'Caldicott Guardian' who will oversee disclosures of patient/client information with particular attention being paid to extraordinary disclosures (those which are not routine). The Caldicott Guardian will oversee the guidance in HSC 2002/003.

This Policy will be reviewed annually, or more frequently if appropriate, to take into account changes to legislation that may occur, and/or guidance from the Department of Health, the Information Commissioner and/or any relevant case law.

7 SUBJECT ACCESS REQUESTS (SARs)

Individuals, Patients or MIP Staff, wishing to exercise any of their rights under GDPR including Subject Access requests, can do so in writing or by emailing governance@medicalimaging.org.uk. These will be responded to inline with MIPs Policy for Processing Subject Access Requests (IG04)

8 SECURITY AND CONFIDENTIALITY

8.1 Data protection by design and default

Data protection issues must be considered from the start of any processing activity, project or system implementation, to ensure the requirements of data protection by design and by default are met through appropriate technical and organisational measures.

This includes:

- minimising the processing of personal data;
- pseudonymising personal data as soon as possible;
- ensuring transparency in respect of the functions and processing of personal data;
- enabling individuals to monitor the processing; and
- creating (and improving) security features.

A Data Protection Impact Assessment will be carried out where processing is "*likely to result in a high risk to the rights and freedoms of natural persons*"

8.2 Security

All information relating to identifiable individuals must be kept secure at all times. MIP will ensure there are adequate procedures in place to protect against unauthorised processing of information and against accidental loss, destruction and damage to this information. Details of how this occurs are within the Information Security Policy.

Measures should be taken to ensure that:

- All software and data is removed from redundant hardware and media storage (e.g. tapes, disks) before the hardware is decommissioned
- Confidential paper waste is shredded or is collected and held in a secure area prior to shredding/incinerating.

8.3 Disposal of confidential waste

MIP has a legal obligation to maintain confidentiality standards for all information relating to patients/clients, employees and business. It is important that this information is disposed of in a secure manner.

All MIP employees will be made aware of how easy it is to breach confidentiality by incorrect use of waste paper, by using examples of 'real life situations' during training sessions. Staff will be informed how to dispose of person-identified waste products.

8.4 Back-ups

The Business Continuity and Disaster Recovery procedure, outlines the media, frequency and retention period for data back-ups.

8.5 Disclosure of information/information in transit

It is important that information about identifiable individuals (such as patients/clients and staff) should only be disclosed on a strict need to know basis. Strict controls governing the disclosure of patient/client identifiable information is also a requirement of the Caldicott recommendations.

Some disclosures of information may occur because there is a statutory requirement upon MIP to disclose e.g. with a Court Order, because other legislation requires disclosure (for staff to the tax office, pension agency and for patients/clients to the Department of Health if the patient/client has a notifiable disease).

Where personal identifiable data is transported via electronic media i.e. CD/DVD, USB memory stick, SD card, all data must be encrypted. Paper documents containing Patient Identifiable data must be sent using recorded delivery.

Contracts between MIP and third parties should include an appropriate confidentiality clause that should be disseminated to third party employees.

9 STAFF AWARENESS AND TRAINING

9.1 Training

All staff will undergo annual data protection and information governance training. This will cover

- Personal responsibilities
- Confidentiality of personal information
- Compliance with the Data Protection Principle
- Individuals rights (access to information and compliance with the principles)
- General good practice guidelines covering security and confidentiality
- A general overview of all information governance components
- General common-sense issues such as locking doors and avoiding discussions in open areas
- A brief overview of how the data protection and freedom of information acts work and the differences

All new starters to MIP will have Information Governance training, to include compliance with the Data Protection Act and general IT security training

A register will be maintained of all staff attendance at training sessions.

All staff will be made aware of what could be classed as an information security incident or breach of confidentiality. They will be made aware of the process to follow and the forms to complete, so that incidents can be identified, monitored and reduced by MIP.

9.2 Reporting Information Security Incidents

All potential information security incidents must be reported in accordance with the requirements of MIP HS03 Incident Reporting Policy and an investigation will be undertaken.

Incidents will be reviewed by the Integrated Governance Committee and Executive Committee. Any major incidents will be immediately reported to the Board where appropriate.

A major incident would constitute a loss of function of a clinical system or breach of confidential information for one or more individuals or a breach of information which is likely to lead to harm to an individual.

9.3 Contracts of employment

Staff contracts of employment are produced by the Chief Operating Officer. All contracts of employment include a Data Protection and general confidentiality clause. Agency and non-contract staff working on behalf of MIP should be subject to the same rules.

All MIP employees will be made aware of their responsibilities in connection with the Acts mentioned in this Policy through their Terms and Conditions, and targeted training sessions carried out by application/system managers and/or other trainers /specialists.

9.4 Disciplinary

A breach of the Data Protection requirements could result in a member of staff facing disciplinary action.

10 AUDIT, MONITORING AND REVIEW

The Clinical Governance Committee will be responsible for leading on the implementation of this policy and other Information Governance related policies and procedures.

This policy will be subject to a regular annual review. The Executive Committee will carry out the review.

An earlier review may be warranted if one of more of the following occurs:

- As a result of regulatory / statutory changes or developments
- As a result of NHS policy changes or developments
- For any other relevant or compelling reason.

11 EQUALITY IMPACT STATEMENT

MIP is committed to ensuring that, as far as is reasonably practicable, the way we provide services to the public and the way we treat our staff reflects their individual needs and does not discriminate against individuals or groups on any grounds. This policy has been assessed accordingly.

1	**Does the policy / guidance affect one group less or more favourably than the other on the basis of:**	**Yes / No**	**Comments**
	• Race	No	
	• Ethnic origins	No	
	• Nationality	No	
	• Gender	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation	No	
	• Age	No	
	• Disability – learning, physical, sensory impairment and mental health problems	No	
2	Is there any evidence that some groups are affected differently?	No	
a	If potential discrimination has been identified, are any exceptions valid, legal and / or justifiable?	No	
3	Is the impact of the policy likely to be negative?	No	
a	If yes, can the impact be avoided?	N/A	
b	What alternatives are there to achieving the policy without the impact?	N/A	
c	Can the impact be reduced by us taking different action?	N/A	

If you identify potential discriminatory impact of this policy, you must refer it to the Governance Lead and the Medical Director along with suggested actions required to reduce or avoid this impact.