



PERINATAL INSTITUTE

CONFIDENTIALITY & DISCLOSURE POLICY

OCTOBER 2004

DOCUMENT CONTROL

Title: Confidentiality & Disclosure Policy

Status: Approved

Version: 2.0

Date Issued: October 2004

Originators: Ann Tonks & Elizabeth Bibby

CONTENTS

Background of the Perinatal Institute	4
Introduction	5
Compliance with relevant legislation and guidance	7
Policy of responsibility	10
Confidentiality	12
Disclosure of information	13
Definitions	15
References	18
Appendix 1	19
Appendix 2	20
Appendix 3	24

BACKGROUND OF THE PERINATAL INSTITUTE

The Perinatal Institute is an NHS organisation core funded by the West Midlands Regional Levy Board and undertaking activities that are supported by the Confidential Enquiry into Maternal And Child Health, the National Screening Committee and the West Midlands Specialised Services Agency.

Its remit is to address the high rate of perinatal mortality and morbidity in the region, and to aid improvements in perinatal care.

This is addressed through:

- Audit of perinatal mortality
- Collection of denominator data (all maternities in region)
- Targeted research
- Collaborative projects to assess service developments
- Dissemination of evidence
- Improvement in training

Other functions of the Perinatal Institute include data collection to support:

- Information for national & regional screening programmes
- Confidential Enquiries
- Epidemiology
- Disease Surveillance
- Commissioning of services
- Audit of equity of service provision
- Audit of levels of patient choice
- Audit of patient safety
- Clinical Governance

This policy has been written to ensure that security and confidentiality is maintained whilst allowing the work of the Perinatal Institute to be carried out practically and efficiently.

INTRODUCTION

This policy covers security of information and data held by the Perinatal Institute (including IT hardware, software and data) and all aspects of confidentiality and disclosure. It incorporates responsibilities of the Perinatal Institute as set out in the following legislation and guidance:

- Protecting and Using Patient Information - A Manual for Caldicott Guardians
- Data Protection Act 1998
- Health and Social Care Act 2001 - Section 60: Control of Patient Information
- Confidentiality: Protecting and Providing Information
- Ensuring Security and Confidentiality in NHS Organisations
- The Perinatal Institute IM&T Policy and Procedures

Scope

This policy covers:

- All staff employed by or contracted with the Perinatal Institute including seconded staff, temporary staff and attached staff (e.g. research associates).
- All personal computers (desktop machines and laptops), attachments and software owned by the Perinatal Institute, whether used at home or within the work place.
- All servers and other hardware and software required to run the networks and information systems.
- All work files and confidential information used by or about employees' and contractors.

Caldicott guidelines cover identifiable data relating to NHS patients. The Data Protection Act covers all identifiable data held on any system (manual or electronic).

Intention

This policy supports procedures that promote security and confidentiality but does not restrict people's ability to work. For example, the need to log off the network when leaving the desk has been weighed against the time taken to log back on. The risk of someone else accessing the network and the likelihood of damage has been considered when devising the policy and security must be appropriate to the risk. Any significant risks identified must be recorded and quantified. All sections of this policy have been written to ensure that security and confidentiality is maintained whilst allowing the work of the Perinatal Institute to be carried out practically and efficiently.

Policy Review

The policy will be reviewed annually or sooner if required. All staff will be informed when the policy is updated. All members of the Perinatal Institute staff will be given a paper copy. The policy is filed on the shared network drive and is available to download from the Perinatal Institute website.

COMPLIANCE WITH RELEVANT LEGISLATION AND GUIDANCE

This policy is based on the recommendations made in the following legislation and publications.

Caldicott Guidelines

These guidelines cover issues surrounding identifiable patient information and specify the need for a Caldicott Guardian to be appointed in all organisations using this type of information.

Professor Jason Gardosi is the Caldicott Guardian for the Perinatal Institute.

Under the guidelines, training must be provided for all staff on an annual basis. This Caldicott training will be combined with discussion around other areas of Information Governance that the Perinatal Institute and the Birmingham and the Black Country Health Authority need to cover or consider.

The Caldicott guidelines also give details of the audit of the confidentiality and security procedures that should be carried out on an annual basis.

Data Protection Act

The Data Protection Act 1998 applies only to living individuals and requires:

- A named lead to manage data protection compliance.
Ann Tonks and Elizabeth Bibby are the named leads for data protection compliance within the Perinatal Institute, working with the Caldicott Guardian.
- Internal training, current awareness, and updates.

The Perinatal Institute is registered under the Data Protection Act:

Registration Number: Z7666186 (expires Feb 2005)

Health and Social Care Act 2001 - Section 60

The Health and Social Care Act brings the issue of informed consent to the fore. It states that to hold and use any patient identifiable data needs the specific informed consent of each patient. There are exemptions covering data that are needed for the public interest and specific cases can be taken to the Secretary of State under Section 60. The legislation is likely to lead "to the use of more anonymised and pseudo-anonymised data sets".

Section 60 of the Health and Social Care Act 2001:

"Enables the Secretary of State to make Regulations for and in connection with requiring or regulating the processing of patient information in prescribed circumstances"

The Act:

- Allows for confidential patient information to be processed without informed consent in support of prescribed activities, such as cancer registries, subject to Regulations which must be agreed by Parliament
- Requires that consistent use of informed consent should be the usual basis for handling confidential patient information
- States that Regulation can provide for processing of patient information for medical purposes where there is benefit to patient care or in the public.
- States that Regulation can only allow processing of information where there is no reasonable alternative
- Requires the Secretary of State to consult with interest groups and also the Patient Information Advisory Group (PIAG) established in December 2001,
- Will require the affirmation of both Houses of Parliament
- States that patient information remains covered by the Data Protection Act 1998 and common law as established in case law.

Of relevance to the Perinatal Institute is Subsection (2) (b), which:

"enables regulations to be made which require the disclosure or other processing of specified patient information subject to conditions or the giving of undertakings. This will support public health work and important activities such as cancer registration where it is essential to maximise the patient information available".

Also of relevance is Subsection (8) that defines patient information as:

"any information that is, or is derived from, information concerning a patient's physical or mental health or condition, the diagnosis of his condition or his care or treatment. In addition to information which directly identifies individuals, this would include information which is either anonymised (e.g. any information that cannot be tracked back to the individual) or coded (e.g. information that can be tracked back to an individual by persons in possession of the key to the code). It includes information recorded in any manner, whether electronically or manually."

Subsection (9) states "confidential patient information", for the purposes of the section, is patient information that has "been obtained by a person who owes an obligation of confidence to an individual where the Identity of that individual is ascertainable from that Information or from that information and other information which is in, or is likely to come into, the possession of the person processing the Information.

General Medical Council Guidance

"Confidentiality: Protecting and Providing Information" places responsibilities upon doctors to:

- Seek patient's consent to the disclosure of information whenever possible
- Anonymised data where unidentifiable data will serve the purpose and
- Keep disclosures to the minimum necessary.

This guidance is in the process of being updated.

BINOCAR Standards on Data Handling

Both the West Midlands Congenital Anomaly Register and the Craniofacial Anomalies Network are affiliated to the British Isles Network of Congenital Anomaly Registers (BINOCAR), and have adopted their additional working practices on data handling - see Appendix 1

Other

There is other legislation that affects information governance, including

- Computer Misuse Act 1990
- Access to Health Records Act 1990
- Human Rights Act 1998
- Freedom of Information Act 2000
- Electronic Communication Act 2000

The Perinatal Institute will keep up to date on any developments in these and other information governance areas.

POLICY OF RESPONSIBILITY

Staff Responsibilities

The Director of the Perinatal Institute has overall responsibility for security and confidentiality issues within the Perinatal Institute.

All the Perinatal Institute staff must receive:

- A copy of the Information Management & Technology Policy & Procedures
- A copy of the Confidentiality & Disclosure Policy

They must read all the policies and sign the Staff Declaration of Compliance, which will be kept in their personnel folder in the Director's office.

Team leaders who manage or supervise staff are responsible for ensuring their staff are aware of the policies and are adhering to them.

Each individual member of staff is personally responsible for ensuring their use of computers, software and confidential information adheres to the policy.

In addition, the following members of staff have the specific roles listed:

- Professor Jason Gardosi (Director) has overall responsibility and for security and confidentiality issues within the Perinatal Institute
- Ms Ann Tonks and Ms Elizabeth Bibby are the named Leads for Data Protection Compliance within the Perinatal Institute and are accountable to the Director
- Mr Stuart Ordish is the IT Systems Manager

Induction & Training

The named leads for Data Protection Compliance will induct new staff so that they are aware of the policy and what actions they need to take to work in line with this policy.

Staff members will be instructed as to their security and disclosure level on commencement of their employment. Access and disclosure rights of information to be reviewed regularly and updated.

All staff will sign an appropriate declaration covering use of laptops and other equipment off site.

The Caldicott Guardian and Leads for Data Protection Compliance will review any updates to the Caldicott or Data Protection requirements.

Training sessions covering the policy will be given annually, or more frequently in the event of significant changes in the policy. All staff must attend these sessions.

Leaving Procedure

Whenever a member of staff leaves, any relevant security system codes should be changed and all keys should be handed in.

The Team leader is responsible for notifying the Perinatal Institute IT administration team that the member of staff is leaving so that all network access will be revoked.

Code of Conduct

All staff of the Perinatal Institute must understand and comply with this policy. They must be aware of the relevant legislation and carry out all work with regard to this policy and the legislation.

Breach of Policy

All Perinatal Institute staff should sign a declaration, which refers to this policy, and this will be binding. Breach of any part of this policy will be a serious disciplinary offence.

- Any breaches of this policy will be reported firstly to one of the Leads for Data Protection Compliance who will then act together with the Caldicott Guardian to ensure the breach ceases
- Anyone suspecting a breach or discovering a situation where a breach could occur should discuss this with the Caldicott Guardian
- Deliberate passing of confidential information to unauthorised people is a disciplinary matter which will lead to dismissal

Internet use is monitored by Birmingham and the Black Country Health Authority. Inappropriate use of the Internet or the sending of inappropriate emails will always result in disciplinary action and may ultimately lead to dismissal. It may also be necessary to proceed with criminal charges depending on the nature of the incident.

CONFIDENTIALITY

Requesting Confidential Information

When requesting confidential information, the request will state who in the Perinatal Institute will hold and process the information and for what purpose the information will be used. Data cannot be used for a different purpose from that for which they were collected.

Storage of Confidential Information

All electronic confidential data must be stored on a server.

No patient data is to be held permanently on the hard disk of personal computers. If it is necessary - temporarily - to store the data on a local hard disk or on magnetic media (e.g. floppy disk, CD) it is the responsibility of the user to ensure that it is password protected and removed or destroyed as soon as possible.

All paper records of confidential information will be stored in a locked filing cabinet in a locked room, when not in use and at the end of the days work.

Use of Confidential Information

When starting to collect a new set of confidential information, the arrangements should be discussed with the Caldicott Guardian. The Caldicott Guardian is responsible for the security and confidentiality of this information.

Details of all confidential databases will be held by the Leads for Data Protection Compliance who will maintain a record of this information.

Access to confidential data will be on a strict need to know basis.

All confidential data must be password protected.

Disposal of Confidential Information

Data (both electronic and paper form) should be disposed of as soon as possible after use. Confidential paper records should not be disposed of in readable form, and should be shredded. Paper used for scrap must not include any personal data.

DISCLOSURE OF INFORMATION

Staff must direct all requests for information to the Caldicott Guardian and must not at any time disclose or release information of any nature unless specifically authorised to do so by the Lead Clinician or Director. All requests for information must be received on the appropriate data request form and be posted/faxed back to the Institute.

Requests for access to data held by the West Midlands Perinatal Institute must include:

- Purpose for which the information is requested
- Justification for the use of the data
- A copy of the Confidentiality & Disclosure Policy for organisations outside the NHS must be supplied. A statement of compliance with the PI security and confidentiality requirements may also be necessary.

In considering requests for access, the Caldicott Guardian will ensure that disclosure is of the minimum data required to meet the purpose and that wherever possible only anonymised data is disclosed.

In all cases

Tables or reports will be devised to minimise the risk of identification from the level of detail appearing in routine reports.

Any demonstrations of the databases should take place using fictitious data.

Control measures to be in place for any output permitting identification of individuals.

Transmissions of information should be restricted as follows:

Mail

- Only supplied to the named individual on the data request form
- Envelopes should be plain (not transit envelopes) and sealed with private and confidential tape
- Address should be marked/stamped as private and confidential
- Media such as CDs or floppy disks must only be used for individuals outside the NHS net
- All media must be password protected and delivered by recorded delivery
- Individuals should be contacted by phone on the day of posting to confirm that the information has been sent with a request to contact the Institute on its arrival
- For media items, the password will be given out to the individual by phone, on receipt

- The individuals will phone the Institute if the information has not been received within 3 working days
- It is the responsibility of the staff member sending out the information to ensure that a record of receipt is kept up-to-date

Email

- Patient identifiable data must sent within encrypted/password protected files over the NHS net only
- The individual must supply their email contact on the data request form
- Once in receipt of the file, the individual must phone to obtain the password
- It is the responsibility of the staff member sending out the information to ensure that a record of receipt is kept up-to-date

Telephone

No confidential information will be given to anyone over the telephone. All requests for information taken over the telephone must be followed up with a written request on the appropriate form.

DEFINITIONS

Confidential information - is defined as:

- Personal details of any patient (e.g. name, address, postcode, telephone number, date of birth) and hospital numbers or other unique identifiers of any health service patient
- Any information pertaining to diagnosis, prognosis or treatment of patients where this is linked to details that may enable the person to be personally identified
- Personal details about employees of the West Midlands Perinatal Institute (e.g. name, address, postcode, telephone number, date of birth)
- Personal details about individuals (e.g. name, address, postcode, telephone number, date of birth).

Confidential Patient Information - is patient information that has been obtained by a person who owes an obligation of confidence to an individual where the identity of the individual is ascertainable from that information or from that information and other information which is in, or is likely to come into, the possession of the person processing the information.

Data Protection Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
 - At least one of the conditions in Schedule 2 is met, and
 - In the case of sensitive personal data, at least one of the conditions in schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Note:

- All purposes are specified and lawful and cover the processing
- Disclosure must be compatible with purposes for which data were obtained.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they were processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

Note:

- Reasonable steps must be taken to ensure accuracy
- Provision must be made for subject's comments in relation to the accuracy of data pertaining to them.

5. Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose or those purposes.

Note:

- Procedures for retention and disposal of records are included in this policy. Data Protection Principles (continued) Patient information.

6. Personal data shall be processed in accordance with the right of data subjects under this Act.

Note:

- Procedures satisfy rights of data subjects.

7. 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.

Note:

- Best practice on information and IT security is covered in this policy.
- There is capability to respond to a breakdown in operations.
- Written contracts are established with all data processors undertaking work for West Midlands Perinatal Institute.

8. Personal data shall not be transferred to a country or territory outside the European Union, 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.

Data Subject - individuals to whom personal data relates.

Data user - person(s) or organisation(s) who controls the contents and use of a collection of personal data (processed, or intended to be processed, automatically).

Disclosure - a disclosure occurs whenever the data or information extracted from the data held are passed (in any format) to someone other than the data user.

Disclosure of Personal Data - occurs when data identifies the data subject or can be used to identify the data subject to whom they relate.

Fair and lawful processing - means that:

- The common law of confidentiality is complied with
- Persons were not misled, deceived or coerced into giving data
- Basic information on users and uses of the data are given
- For health data, the conditions in schedules 3 are applied
- Data sharing protocols in response to Caldicott guidelines must also comply with the Data Protection Act
- Data subjects should usually be informed about the identity of the data controller and uses of the data.

Patient Information - any information that is, or is derived from, information concerning a patient's physical or mental health or condition, the diagnosis of his condition or his care or treatment. In addition to information that directly identifies individuals, this would include Information that is either anonymised (e.g. any information that cannot be tracked back to the individual) or coded (e.g. information that can be tracked back to an Individual by persons in possession of the key to the code). It includes information recorded in any manner, whether electronically or manually.

Personal data - data consisting of information that relates to a living individual who can be identified from that information (or from that and other information in the possession of the data user).

REFERENCES

NHS Executive's Security And Data Protection Programme. Ensuring Security and Confidentiality in NHS Organisations. NHS Information Authority, 1999.

Information Management & Technology Policy & Procedures. Perinatal Institute March 2004

Walker P. Protecting and Using Patient Information - a Manual for Caldicott Guardians. NHS Executive, 1999.

Data Protection Act 1998 - Chapter 29. The Stationery Office, 1998.

Health and Social Care Act 2001 - Chapter 15. The Stationery Office, 2001.

General Medical Council. Confidentiality: Protecting and Providing Information. General Medical Council, 2000.

Human Rights Act 1998 - Chapter 42. The Stationery Office, 1998.

Freedom of Information Act 2000 - Chapter 36. The Stationery Office, 2000.

Electronic Communications Act 2000 - Chapter 7. The Stationery Office, 2000.

Confidentiality: NHS Code of Practice 2003 <http://www.doh.gov.uk/ipu/confiden>

Further information can be found in G:\INFORMATION GOVERNANCE

APPENDIX 1

BINOCAR STANDARD ON DATA HANDLING

All paper/electronic information, and back up tapes are kept in locked cupboards in locked rooms in secure buildings

All computer information are stored on password protected dedicated systems with no outside links

No identifiable information is sent over email or fax

The issue of confidentiality is central in the interview for any job working on a register and is addressed regularly with staff

Strict guidelines protecting confidentiality are adhered to regarding the use of data by those doing research, no identifiable information is published

Registers are inspected by a governing body to ensure that high standards exist and are maintained.

APPENDIX 2

DATA PROTECTION PRINCIPLES

First principle - Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless -

- (a) at least one of the conditions in Schedule 2 is met, and
- (b) in the case of sensitive personal data at least one of the conditions in Schedule 3 is also met.

SCHEDULE 2

1. The data subject has given his consent to the processing.
2. The processing is necessary -
 - a) for the performance of a contract to which the data subject is a party, or
 - b) for the taking of steps at the request of the data subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
4. The processing is necessary in order to protect the vital interests of the data subject.
5. The processing is necessary:
 - a) for the administration of justice,
 - b) for the exercise of any functions conferred on any person by or under any enactment,
 - c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
 - d) for the exercise of any other functions of a public nature exercised in the public interest by any person.
6. (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.
(2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, taken to be satisfied.

SCHEDULE 3

1. The data subject has given his explicit consent to the processing of personal data.
2. (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

(2) The Secretary of State may by order -

- a) exclude the application of subparagraph (1) in such cases as may be specified, or
 - b) provide that, in such cases as may be specified, the condition in subparagraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
3. The processing is necessary -
- a) in order to protect the vital interests of the data subject or another person, in a case where -
 - i. consent cannot be given by or on behalf of the data subject, or
 - ii. the data controller cannot reasonably be expected to obtain the consent of the data subject, or
 - b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.
4. The processing -
- a) is carried out in the course of its legitimate activities by any body or association which -
 - i. is not established or conducted for profit, and
 - ii. exists for political, philosophical religious or trade union purposes.
 - b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
 - c) relates only to individuals who either are members of the body association or have regular contact with it in connection with its purposes, and
 - d) does not involve disclosure of the personal data to a third party without the consent of the data subject.
5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.
6. The processing:
- a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings)
 - b) is necessary for the purpose of obtaining legal advice, or
 - c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
7. 1) The processing is necessary
- a) for the administration of justice.
 - b) for the exercise of any functions conferred on any person by or under an enactment, or
 - c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

- 2) The Secretary of State may by order
 - d) exclude the application of subparagraph (1) in such cases as may be specified, or
 - e) provide that, in such cases as may be specified, the condition in subparagraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
8. (1) The processing is necessary for medical purposes and is undertaken by
 - a) a health professional, or
 - b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.
 - c) (2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.
9. (1) The processing -
 - a) is of sensitive personal data consisting of information as to racial or ethnic origin,
 - b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained and,
 - c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.
 - d) (2) The Secretary of State may be order specify circumstances in which processing falling within the sub paragraph (1) (a) and (b) Is, or is not, to be taken for the purposes of sub paragraph (1) (c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.
10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.

Second principle – Personal data can shall be obtained only for one or more specific and lawful purpose 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 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.

APPENDIX 3

CALDICOTT PRINCIPLES

The Chief Medical Officer established the Caldicott Committee in England to review the passage of patient identifiable information. Its purpose was to ensure that patient identifiable information is only transferred for justifiable purposes and that only the minimum necessary information is transferred in each case. The Committee reported on 10th December 1997 and published a set of 6 guiding principles:

1. **Justify the purpose(s)** - Every proposed use or transfer of patient identifiable information within or for an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.
2. **Don't use patient identifiable information unless it is absolutely necessary** - Patient identifiable information items should not be used unless there is no alternative.
3. **Use the minimum necessary patient identifiable information** - Where use of patient identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiability.
4. **Access to patient identifiable information should be on strict need to know basis** - Only those individuals who need access to patient Identifiable information should have access to it, and they should only have access to the information items that they need to see.
5. **Everyone should be aware of their responsibilities** - Action should be taken to ensure that those handling patient identifiable information, both clinical and non-clinical staff, are aware of their responsibilities and obligations to respect patient confidentiality.
6. **Understand and comply with the law** - Every use of patient identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.



STAFF DECLARATION OF COMPLIANCE TO CONFIDENTIALITY & DISCLOSURE POLICY

I understand that in the course of my work, I may encounter, or have access to, confidential information relating to individual patients or NHS staff. I understand that misuse of this information, especially its disclosure to people or agencies that are not authorised to receive it, would constitute a serious breach of confidentiality.

I have read and understood the West Midlands Perinatal Institute Confidentiality and Disclosure Policy. I understand that failure to adhere to the policy may lead to disciplinary action.

I also understand that intentional divulgence of identifiable patient information in breach of this policy will lead to disciplinary action, which may involve dismissal.

I understand that the use and security of personal information is subject to the provisions of the Data Protection Act 1998 and that unauthorised disclosure of personal information is a criminal offence under the Act.

Name: _____

Title: _____

Signed: _____

Date: _____