Milton Keynes University Hospital NHS Foundation Trust

Policy **Data Subject Access & Individual Rights Policy**	
Classification :	Policy
Authors Name:	Dawn Budd
Authors Job Title:	Information Governance Manager
Authors Division:	Corporate
Departments/ Group this Document applies to:	All
Date of Approval: October 2018	Review Date: October 2021
Approval Group: Information Governance Steering Group, Documentation Committee	Last Review:

Unique Identifier: to be allocated	**Status:** Draft	**Version No:** 1
Policy to be followed by (target staff): All staff groups		
To be read in conjunction with the following documents: The Data Protection Act 2018 incorporating GDPR The Trust's Access to Health Records Application Form Information Governance policy Information Governance strategy		
CQC Fundamental standards: Regulation 17 – Good governance Regulation 19 – Fit and proper		

Index

1. Introduction

A Subject Access Request is a request from an individual asking an organisation to provide them with information relating to that person which is held or processed by the organisation.

The person requesting the data does not need to give a reason for wanting access however they only have a right to see information about themselves (data subject).

1.1 Data Protection Act 2018/ General Data Protection Regulations (GDPR) here after known as the act.

Individuals have several rights in relation to the information held about them. Access gives them the right to obtain a record in permanent form.

The act states that individuals (Identifiable Natural Person) have a right to obtain confirmation as to whether or not personal data concerning them is being processed, and where that is the case to have access to that personal data.

The Individual can access the data held about them by making a request in writing or verbally for a copy of the information the Trust holds both in electronic format and paper.

1.2 Access to Health Records Act 1990 (ATHR)

This Act has been repealed to the extent that it only relates to the health records of deceased patients. It applies only to records created since 1st November 1991. Applications for disclosure of records for deceased patients should only be granted to the personal representative of the estate or to someone having a claim arising out of the death.

While there is no legal entitlement other than the limited circumstances covered under the Access to Health Records legislation, health professionals have always had discretion to disclose information to a deceased person's relatives or others when there is a clear justification. A common example is when the family requests details of the terminal illness because of an anxiety that the patient might have been misdiagnosed or there might have been negligence. Disclosure in such cases is likely to be what the deceased person would have wanted and may also be in the interests of justice. Refusal to disclose in the absence of some evidence that this was the deceased patient's known wish exacerbates suspicion and can result in unnecessary litigation. In other cases, the balance of benefit to be gained by the disclosure to the family, for example of a hereditary or infectious condition, may outweigh the obligation of confidentiality to the deceased.

2. Scope

This policy deals with the rights of Data Subjects whereby individuals can request access to their personal data.

This policy applies to all requests for access to personal data held by the Trust. This applies to anyone about whom the Trust holds information – including staff, ex-staff, patients, service users and other agencies.

This policy provides a framework for the Trust to ensure compliance with the Act and Access to Health Records Act 1990.

This policy is supported by operational procedures and activities as detailed in appendices 1-3.

3. Definitions

Data Protection Act 2018 / GDPR	The Data Protection Act / GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data. Personal data that has been pseudo-anonymised – e.g. keycoded – can fall within the scope of the The Data Protection Act / GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.
Personal Identifiable Information (PII)	Any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. The Act definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.
Special Category Personal data	The special categories include, racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data where processed to uniquely identify an individual, data concerning health or data covering and individual's sex life or sexual orientation. Personal data relating to criminal convictions and offences are not included, but safeguards apply to its processing.
Identifiable Natural Person (INP)	The person the information is about and who can be identified from that information. All Identifiable Natural Persons have certain legal rights in relation to their personal identifiable information
Health Record	A 'health record' is defined as being any record which consists of information relating to the physical, mental or condition of an individual, and has been made by a health professional in connection with the care of that individual. The definition can also apply to material held on an x-ray or an MRI scan. This means that when a subject access request is made, the information contained in such material must be supplied to the applicant.
Employment Record	An 'employment record' is defined as being any record which consists of information relating to a current or former member of staff and has been made by or on behalf of the Trust in connection

	with the individual's employment.
Occupational Health Record	An 'occupational health record' is defined as being any record which consists of information relating to the physical or mental or condition of a current or former member of staff and has been made in connection with the individual's employment.
Complaint File	A 'complaint file' is defined as being any record which consists of information relating to a complaint made by a patient or a representative acting on their behalf.
Incident File	An 'incident file' is defined as being any record which consists of information relating to an incident involving a patient; employee; contractor or visitor.

4. Roles and Responsibilities

Caldicott Guardian - The Caldicott Guardian has a strategic role, developing security and confidentiality of patient information and to facilitate sharing where appropriate, and for representing confidentiality requirements and issues at Board level.

Data Protection Officer
A Data Protection officer (DPO) is a leadership role required by the Data Protection Act 2018 /General Data Protection Regulations (GDPR). Data protection officers are responsible for overseeing the data protection strategy and implementation to ensure compliance with GDPR requirements

The controller and the processor need to involve the DPO fully and at the earliest point in all issues which relate to the protection of personal data.

A consultative and Advisory Role to include the following:-

- Monitor Trust Compliance with the Act
- Provide advice on DPIA's including the need to undertake one
- Investigate and report to the ICO all breaches within 72 hours (if a person's right is infringed)
- Undertake record keeping functions
- Independent and cannot be instructed to the output of advice

The Information Governance Manager has responsibility for ensuring all Subject Access Requests regarding health records, complaints and employees are actioned.

The Complaints Manager has responsibility to forward all Subject Access Requests regarding complaints to the Information Governance Manager.

The Head of Risk and compliance has responsibility for ensuring all Subject Access Requests regarding patient safety incidents and alerts are actioned.

The Head of Human Resources is responsible for compiling the information in response to requests by employees or ex-employees for copies of their personal employment files (this includes both medical and non-medical staff) and forwarding a copy of the information to the Information Governance manager to facilitate.

All managers must ensure their staff are aware of this policy and procedure and know how to deal with requests for personal/patient identifiable information.

5. Who can make an application for personal data?

- The Data Subject
- A person lawfully acting on their behalf:
  - Their lawyer with consent form
  - Person with parental responsibility for under 13s
  - Person with authority to manage affairs of an incapacitated adult [Refer to Mental Capacity Act]
  - Police and other agencies

Where the patient is deceased, the relevant authority must be provided.

6. Timescales

It is important that action is taken promptly as the legislation dictates that the information must be provided without delay and at the latest within one month of receipt of the request.

The timescale for the period of compliance may be extended by a further two months where requests are complex or numerous. If this is the case, the individual must be informed immediately giving them an explanation given as to why the extension is necessary.

7. Charges

A copy of the information must be provided free of charge. However, when a request is manifestly unfounded or excessive, particularly if it is repetitive a 'reasonable fee' can be charged.

A reasonable fee can be charged to comply with requests for further copies of the same information.

The fee must be based on the administrative cost of providing the information.

8. Provision of the Information Requested

The identity of the person making the request must be verified using 'reasonable means'. If the request is made electronically, where possible the information should be provided in a commonly used electronic format.

8.1 Requests for large amounts of personal data

Where a large quantity of information is processed about an individual, the Act permits the Trust to ask the individual to specify the information the request relates to.

The Act does not include an exemption for requests that relate to large amounts of data, but the Trust may be able to consider whether the request is manifestly unfounded or excessive (see 8.3 below).

8.2 The Duty to Search

Searches need to be reasonable and proportionate. The coordinator dealing with the request must be able to provide a log to show what searches have been undertaken in line with the request.

8.3 Manifestly unfounded or excessive requests

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, the Trust can:

- Charge a reasonable fee taking into account the administrative costs of providing the information, or Refuse to respond.

Where the decision is made to refuse to respond to a request, an explanation of the reason must be given to the individual, informing them of their right to complain to the Information Commissioners office. The individual should be informed of the decision without undue delay and at the latest within one month of receipt of the request.

Advice should be sought from the Data Protection Officer.

9. Rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

If the personal data in question has been disclosed to others, each recipient must be contacted and informed of the rectification - unless this proves impossible or involves disproportionate effort. If asked, the individual must be informed about these recipients.

Where the Trust does not take action in response to a request for rectification, it must explain why to the individual informing them of their right to complain to the Information Commissioners Office.

9.1 Timescale to comply with a request for rectification

A response to a request for rectification must be complied with within one month of receipt of the request. This can be extended by two months where the request for rectification is complex.

If a decision is taken not to take action in response to a request for rectification, an explanation as to why must be given to the individual, informing them of their right to complain to the Information Commissioner and to a judicial remedy.

Advice should be sought from the Data Protection Officer.

10.0 The Right to Erasure (the right to be forgotten)

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the ActT).
- The personal data has to be erased in order to comply with a legal obligation.

If the processing does cause damage or distress, this is likely to make the case for erasure stronger.

There are some specific circumstances where the right to erasure does not apply and you can refuse to deal with a request.

10.1 When can I refuse to comply with a request for erasure?

The Trust can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority
- for public health purposes in the public interest
- archiving purposes in the public interest, scientific research historical research or statistical purposes, or
- The exercise or defense of legal claims.

10.2 How does the right to erasure apply to children's personal data?

There are extra requirements when the request for erasure relates to children's personal data, reflecting the Act emphasis on the enhanced protection of such information, especially in online environments.

The Trust must pay special attention to existing situations where a child has given consent to processing and they later request erasure of the data (regardless of age at the time of the request), especially on social networking sites and internet forums. This is because a child may not have been fully aware of the risks involved in the processing at the time of consent.

10.3 Do I have to tell other organisations about the erasure of personal data?

If the Trust has disclosed the personal data in question to third parties, they must be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

11. The right to restrict processing

The Trust is required to restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.
-
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether the Trust's legitimate grounds override those of the individual.

- When processing is unlawful and the individual opposes erasure and requests restriction instead.

- If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

If the Trust has disclosed the personal data in question to third parties, you must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

12. The right to object

The Trust must recognise that individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and

Processing for purposes of scientific/historical research and statistics.

12.1 If an Individual has a right to object to the Trust processing their information on "grounds relating to his or her particular situation".

You must stop processing the personal data unless:

you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
the processing is for the establishment, exercise or defence of legal claims.

The Trust ensures that the right to object is written into its privacy notice.

13. Subject Access Requests Process

See appendix 1 SAR Standard Operating Procedure

Requests will be monitored through reporting to the Information Governance Steering Group

(IGSG)

14. Implementation

The Information Governance manager and team will raise awareness of the policy in relevant training sessions and meetings.

The Information Governance Officer will ensure access to records are logged and processed to meet the required timescales for completion.

Staff involved with requests must be trained and be aware of the process to ensure they respond to meet the requirements and timescales detailed in the policy.

14.1 Dissemination

This policy will be published on the Trust's Intranet. It is the responsibility of line managers to ensure that members of staff are made aware of this policy. New members of staff are advised during their induction process to look at the Trusts Internet and Intranet to ensure that they read and have a good working knowledge of all relevant policies, strategies, procedures and guidelines.

15. Training and awareness

Annual Data Awareness training is mandatory for all staff. Any staff responsible for handling Subject Access requests must be aware of their responsibilities for complying with this policy.

16 Governance

16.1 Document review history

Version number	Review date	Reviewed by	Changes made
1			

16.2 Consultation History

Stakeholders Name/Board	Area of Expertise	Date Sent	Date Received	Comments	Endorsed Yes/No
Information Governance Department	Information Governance			New Policy	
IGSG	Information Governance			Minor amendments	
Compliance and Audit Manager	Compliance				
Documentation Committee					

16.3 Audit and monitoring

Audit/Monitoring Criteria	Tool	Audit Lead	Frequency of Audit	Responsible Committee/Board
Compliance with General Data Protection Regulations May 2018	Electronic/ Manual Audits	Data Protection Officer	Quarterly	Information Governance Steering Group & Audit Committee
Compliance with Access to Health Records Act 1990	Electronic/ Manual Audits	Data Protection Officer	Quarterly	Information Governance Steering Group & Audit Committee
IG Toolkit	Electronic/ Manual Audits	Data Protection Officer	Quarterly	Information Governance Steering Group & Audit Committee

16.4 Equality Impact Assessment

As part of its development, this policy and its impact on equality has been reviewed. The purpose of the assessment is to minimise and if possible remove any disproportionate impact on the grounds of race, gender, disability, age, sexual orientation, religion or belief, pregnancy and maternity, gender reassignment or marriage and civil partnership. No detriment was identified.

Equality Impact Assessment			
Division	**Corporate**	**Department**	**Information Governance**
Person completing the EqIA	Data Protection Manager	**Contact No.**	**85041**
Others involved:		**Date of assessment:**	**22 December 2017**
Existing policy/service	Change of Policy with new Act	**New policy/service**	**New Policy**
Will patients, carers, the public or staff be affected by the policy/service?	Staff /patients		
If staff, how many/which groups will be effected?	All staff and patients		
Protected characteristic	**Any impact?**	**Comments**	
Age	NO		

Disability	NO	
Gender reassignment	NO	
Marriage and civil partnership	NO	
Pregnancy and maternity	NO	
Race	NO	
Religion or belief	NO	
Sex	NO	
Sexual orientation	NO	
What consultation method(s) have you carried out?		
How are the changes/amendments to the policies/services communicated?		**Via training, intranet and news bulletins**

Milton Keynes University Hospital NHS Foundation Trust

APPENDIX 1

Standard Operating Procedure (SOP) Number: 1

SOP Title: Subject Access Requests

Classification :	Standard Operating Procedure
Authors Name:	**Dawn Budd**
Authors Job Title:	**Information Governance Manager**
Authors Division:	**Information Governance**
Departments/Groups This Document Applies to: All Staff	
Date of Approval:	**Review Date: 1st June 2019**
Approval Group: Information Governance Steering Group	**Last Review: 1st May 2018**
Approval Signature:	

Status: Final	**Version No: 1**
Scope: All staff	**Document for Public Display:** No
To be read in conjunction with the following documents: N/A	

Record of changes to document

Version number: 1		**Date:** 1st May 2018		
Section Number	**Amendment**	**Deletion**	**Addition**	**Reason**

1. Introduction

The GDPR brings with it new laws surrounding Subject Access with shorter timescales and fees being abolished. The Trust receives around 150 plus records per month from the following areas:

- In-patient
- Patients
- Solicitors
- Police
- Agencies
- Relatives
- Social Services
- DWP
- Other Agencies
- GMC

The Trust must ensure that all Subject Access Requests are dealt with in an efficient and timely manner in line with the Data Protection Act 2018/General Data Protection Regulations (GDPR)

2. Purpose

The purpose of this document is to lay down the timescales and procedure for all subject access requests to ensure that the Trust meet the deadlines.

3. Responsibilities

Information Governance Manager
It is the responsibility of the Information Governance Manager to manage and oversee the Subject Access Request process and to ensure that the Trusts meet the current timescales laid down and follows current legislation in all responses.

Information Governance Officers
It is the responsibility of the Information Governance Officers to co-ordinate all the requests and liaise directly with the requester and keep them up to date with the state of their request.

Data Protection Officer
It is the Data Protection Officer role to ensure that all breaches of legislation are identified, investigated and actions implemented in line with the findings.

All Staff
It is the responsibility of all staff to identify a subject access request and forward it to the Information Governance Department in a timely manner.

4. How to recognize a request

The Data Protection Act does not specify how to make a valid request. Therefore, an individual can make a subject access request verbally or in writing. It can also come in to any part of the hospital. A subject access request (SAR) is simply a written request made by or on behalf of an individual for the information which he or she is entitled to ask for. A SAR must be made in

writing and although the Trust has a Standard form which makes it easier for us to recognise there is no legally prescribed request form and they do not have to use it. The request does not have to be in any particular form. Nor does it have to include the words 'subject access' or make any reference to the Data Protection Act. An emailed or faxed request is as valid as one sent in hard copy. SARs might also be received via social media and possibly via third-party websites.

All requests must be passed to the Information Governance department within 1 day of receipt.

5. Procedure

All requests are different and will vary in the amount of information requested, the age and complexity. The Trust has many systems that may need to be integrated to identify data requested. Data may also need to be redacted before disclosure.

- Identify individual and information requested
- Requests will be logged onto the Trust database which calculates the timescales.
- Information will be requested from various departments i.e. imaging, medical records, off site storage, various patient systems.
- Information will be put on disc or printed whichever is the preference
- Redactions will be made where necessary
- Information will be sent out via recorded/tracked delivery or collected by the requested, whichever the preference.

6. Timescales

The Trust abides by the current timescale laid down of one calendar month but aims to supply the requested information within 21 days NHS best practice. The Trust meets this target on 95% of requests. Some of the more complex requests will take longer but the patient is always informed and a dialogue held of the reasons for this e.g.

- Requester thinks documentation is missing
- Complexity of the request – manifestly unfounded
- Information held on an archived system or storage
- Lack of correct documentation by the requester

Milton Keynes University Hospital NHS Foundation Trust

APPLICATION FOR ACCESS TO HEALTH RECORDS
(By the Patient)

DATA PROTECTION ACT 2018 INCORPORATING THE GENERAL DATA PROTECTION REGULATIONS 2018

IN CONFIDENCE

Please read the Information Notes prior to completing this form in ink using block capitals. On completion return to:

Access to Health Records Dept, Milton Keynes University Hospital NHS Foundation Trust, Standing Way, Eaglestone, Milton Keynes, MK6 5LD

Accesstohealthrecords@mkuh.nhs.uk

HOSPITAL NO: _____

Surname:_____ Former/MaidenName: _____

Forenames:_____ Date of Birth: _____

Current Address: _____

Postcode: _____ Telephone: _____

Previous Address: _____

Email Address: _____

IS THIS APPLICATION PART OF A COMPLAINT?

YES ☐ NO ☐

WHICH OF THE FOLLOWING DO YOU REQUIRE?

Medical Records: Yes ☐ No ☐ Accident & Emergency: Yes ☐ No ☐

X-Rays/Scans/Images: Yes ☐ No ☐ Blood Test Results: Yes ☐ No ☐

Please Be Aware That X-Rays Will Be On Disc

Please state what form you would like your medical notes in:

Paper copy ☐ Disc ☐ Email ☐

(Please note emails will be sent encrypted and you will need to call the Access to Health Records office to obtain the password)

COMMENTS (Please provide any relevant information to help us identify the records you require)

Milton Keynes University Hospital NHS Foundation Trust

DISCLOSURE OF INFORMATION

Please read the Information Notes prior to completing this form in ink using block capitals

DECLARATION

I declare that the information given in this form is correct, to the best of my knowledge and:

As proof of my identity I attach a copy of my:

Photo ID and Proof Of address (E.G Driving Licence/Passport & Utility Bill/Bank Statement)

Signed: _____ Print Name: _____

Date: _____

WARNING

You are advised that the making of false or misleading statements in order to obtain access to personal information to which you are not entitled is a criminal offence.

Milton Keynes University Hospital NHS Foundation Trust

APPLICATION FOR ACCESS TO HEALTH RECORDS
(On behalf of the child by the Parent/Guardian)

DATA PROTECTION ACT 2018 INCORPORATING THE GENERAL DATA PROTECTION REGULATIONS 2018

IN CONFIDENCE

Please read the Information Notes prior to completing this form in ink using block capitals. On completion return to:

Access to Health Records Dept, Milton Keynes University Hospital NHS Foundation Trust, Standing Way, Eaglestone, Milton Keynes, MK6 5LD

Accesstohealthrecords@mkuh.nhs.uk

HOSPITAL NO: _____

Surname:_____ Former/MaidenName: _____

Forenames:_____ Date of Birth: _____

Current Address: _____

Postcode:_____ Telephone: _____

Previous Address: _____

Email Address: _____

IS THIS APPLICATION PART OF A COMPLAINT?

YES ☐ NO ☐

WHICH OF THE FOLLOWING DO YOU REQUIRE?

Medical Records: Yes ☐ No ☐ Accident & Emergency: Yes No ☐ ☐

X-Rays/Scans/Images: Yes ☐ No ☐ Blood Test Results: Yes ☐ No ☐

Please Be Aware That X-Rays Will Be On Disc

Please state what form you would like your medical notes in:

Paper copy ☐ Disc ☐ Email ☐

COMMENTS (Please provide any relevant information to help us identify the records you require)

Milton Keynes University Hospital NHS Foundation Trust

DISCLOSURE OF INFORMATION

Please read the Information Notes prior to completing this form in ink using block capitals

DECLARATION

I declare that the information given in this form is correct, to the best of my knowledge, and that:

I am the parent/guardian of the person named overleaf.

As proof of my identity and responsibility of the patient/child I attach a copy of my:
Photo ID and Proof of Address (E.G Driving Licence/Passport & Utility Bill/ Bank Statement)

As proof of the patient/Childs Identity I attach a copy of their:

- Birth Certificate

And Proof of Address (Only one needed):

- Recent Correspondence – no longer than 3 months old
- Letter from doctor/hospital
- Child Benefit book/letter

Signed: _____ Print Name: _____

Date: _____

WARNING

You are advised that the making of false or misleading statements in order to obtain access to personal information to which you are not entitled is a criminal offence.

Milton Keynes University Hospital NHS Foundation Trust

APPLICATION FOR ACCESS TO DECEASED RECORDS IN CONFIDENCE

Please read the Information Notes prior to completing this form in ink using block capitals. On completion return to:

Access to Health Records Dept, Milton Keynes University Hospital NHS Foundation Trust, Standing Way, Eaglestone, Milton Keynes, MK6 5LD

Accesstohealthrecords@mkuh.nhs.uk

Please fill out the deceased patient's details below

HOSPITAL NO: _____

Surname:_____ Former/Maiden Name: _____

Forenames: _____

Date of Birth: _____

Last Known Address: _____

Postcode:_____

IS THIS APPLICATION PART OF A COMPLAINT?

YES ☐ NO ☐

WHICH OF THE FOLLOWING DO YOU REQUIRE?

Medical Records: Yes ☐ No ☐ Accident & Emergency: Yes ☐ No ☐

X-Rays/Scans/Images: Yes ☐ No ☐ Blood Test Results: Yes ☐ No ☐

Please Be Aware That X-Rays Will Be On Disc

Please state what form you would like your medical notes in:

Paper copy ☐ Disc ☐ Email ☐

COMMENTS (Please provide any relevant information to help us identify the records you require)

Milton Keynes University Hospital NHS Foundation Trust

DISCLOSURE OF INFORMATION

Please read the Information Notes prior to completing this form in ink using block capitals.

CERTIFICATION

Please fill out your details below

I certify that I am (Name):_____

Of (address): _____

_____ Tel No: _____

Please provide the following forms of ID below in your application:

1. Access by the executor/Patient representative

- Photo ID
- Proof of address
- Death Certificate
- Proof of executor

2. Claim arising from Estate

- Photo ID
- Proof of address
- Evidence of claim

3. Miscellaneous

- Photo ID
- Proof of address
- Dr to request if medical reason for family history etc.
- Seek permission of IG manager.

Signed: _____ Print Name: _____

Date: _____

WARNING

You are advised that the making of false or misleading statements in order to obtain access to personal information to which you are not entitled is a criminal offence.