Trust Policy

University Hospitals Plymouth NHS Trust

Subject Access Request (SAR) Policy

Issue Date	Review Date	Version
August 2018	Extended to January 2020	2

Purpose

To outline how access requests for personal information will be managed by the Trust in accordance with Legislation listed in Section 2.

Who should read this document?

All staff.

Key Messages

A Subject Access Request (SAR) can be received by anyone within the Trust. If you receive a SAR this MUST be sent to the Disclosure Team immediately for them to action. All SARs MUST be completed within 30 calendar days of receipt; otherwise the Trust will breach the target.

All SARs are processed by the Disclosure Team and they will determine what information is disclosed by following approved processes.

Core accountabilities	
Owner	Central Records Library Manager
Review	Caldicott and Information Governance Committee (CIGAC) and the Integrated Digital Care Record Board (IDCR)
Ratification	Senior Information Risk Owner (SIRO)
Dissemination	Head of Health Records and eNotes Implementation
Compliance	Central Records Library Manager reports to Caldicott and Information Governance Assurance Committee (CIGAC)

Links to other policies and procedures

Data Protection Policy

Information Governance Policy

Information Governance Management Framework

Recording of Patients' Wishes regarding the Management of their Personal Data Administrative Procedure Note (APN)

Management of Freedom of Information (FOI) Requests Standard Operating Procedure (SOP)

Version History		
1	August 2018	Initial Document
2	November 2019	Extended to January 2020

The Trust is committed to creating a fully inclusive and accessible service. Making equality and diversity an integral part of the business will enable us to enhance the services we deliver and better meet the needs of patients and staff. We will treat people with dignity and respect, promote equality and diversity and eliminate all forms of discrimination, regardless of (but not limited to) age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage/civil partnership and pregnancy/maternity.

An electronic version of this document is available on Trust Documents on StaffNET. Larger text, Braille and Audio versions can be made available upon request.

Contents

1. Introduction

1.1 This Policy details how University Hospitals Plymouth NHS Trust will manage Subject Access Requests (SARs) effectively. It covers requests for access to all personal information, from whatever source, to Trust's Records.

1.2 This policy aims to unify procedures across the Trust in complying with all relevant legislation in respect of SARs.

2. Purpose, including legal or regulatory background

2.1 Individuals have a right to access their own health records, and in limited circumstances, access to the records of other people. Requests can also be received from Trust Staff asking for access to their personnel/employee records. Requests for access to personal information held by the Trust are becoming more commonplace. It is therefore necessary to put into place a policy and procedure for dealing with such requests in order to ensure access is given promptly, appropriately and in compliance with the following Legislation:

- The Data Protection Act 2018 from 25th May 2018 (DPA)
- The General Data Protection Regulation (GDPR) (from 25th May 2018)
- The Access to Health Records Act 1990 (AHRA) (for deceased patients)
- The Access to Medical Reports Act 1988
- The Human Rights Act
- The Freedom of Information Act
- Confidentiality: NHS Code of Practice
- The NHS Care Record Guarantee
- ICO Codes of Practice
- Records Management Code of Practice for Health and Social Care 2016

The Information Commissioners Office (ICO) is the independent regulator of the Data Protection Act, the General Data Protection Regulation (from 25th May 2018) and the Freedom of Information Act in England and Wales. The ICO can issue sanctions against any organisation should they breach the Acts or the Data Subjects' rights.

3. Scope

Any individual working in the Trust could receive an SAR and will be required to manage the request appropriately therefore this Policy is applicable to all staff across University Hospitals Plymouth NHS Trust.

4. Definitions

4.1 **A Subject Access Request (SAR)**

- This is a request from an individual or organisation asking that the Trust provides them with the information, relating to an individual, which is held or processed by the Trust.

- These are normally requests for Medical or Staff Personnel Records held by the Trust on a patient or staff member by the individual or by their personal representative or solicitor.

4.2 **The Health Record**

The DPA 1998, describes the **Health Record** as:
'Consisting of information about the physical and mental health or condition of an identifiable individual made by or on behalf of a health professional in connection with the care of that individual'.

The British Medical Association (BMA) defines a **Health Record** as:
'Any record which consists of information relating to the physical or mental health or condition of an individual made by a health professional in connection with the care of that individual. It can be recorded in a computerised form, in a manual form or a mixture of both. Information covers expression of opinion about individuals as well as fact. Health records may include notes made during consultations, correspondence between health professionals such as referral and discharge letters, results of tests and their interpretation, X-ray films, videotapes, audiotapes, photographs, and tissue samples taken for diagnostic purposes. They may also include internal memoranda, reports written for third parties such as insurance companies, as well as theatre lists, booking-in registers and clinical audit data, if the patient is identifiable from these'.[1]

The list above is not exhaustive but does show the breadth of information that should be considered when responding to a SAR.

4.3 **Personal Data/Information** is defined by the ICO as below:

- Personal data means data which relates to a living individual who can be identified from that data, or
- from the data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

4.4 **Personal Representative**

Relevant to requests for access to deceased patient records, they are defined as:

- the person named in the will of a deceased patient as their executor, or
- a person appointed as the administrator of the deceased person's estate.

[1] BMA Access to health records Guidance for health professionals in the United Kingdom. August 2014

4.5 The Data Protection Legislation

From the 25th May 2018 the main piece of legislation is the Data Protection Act 2018 (DPA). This policy is based on the Subject Access Rights defined by the DPA and by the strengthening of these rights as set out in the General Data Protection Regulation.

The DPA regulates the processing of personal data about living identifiable individuals. It applies to all personal data, not just to health records. Similarly, it is not confined to health records held for the purposes of the NHS. It applies equally to social care records, the private health and care sector and to health professionals' private practice records (for example those of psychiatrists, podiatrists, therapists). The same principles also apply to records of employees held by employers, for example in finance, personnel and occupational health departments.

Processing includes obtaining, holding, using or disclosing of such information. The Act also provides individuals with a right to apply for access to information which is held in their records. Identifiable information should be processed in accordance with the 8 Data Protection Principles.

4.6 The General Data Protection Regulation (GDPR)

GDPR is a new EU law that came into effect on the 25th May 2018. This regulation is part of the updated Data Protection Act 2018. The GDPR will give individuals greater rights over their personal information. The ICO have published a 'Guide to GDPR'. On page 52 under 'Right of Access' it states the following regarding the change in fees:

- You must provide a copy of the information **free of charge**. However, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.
- You may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests.
- The fee must be based on the administrative cost of providing the information.
- The timescale to complete these requests will also be reduced to within one month (30 calendar days) from the current target of 40 calendar days.

4.7 The Access to Health Records Act 1990 (AHRA)

The AHRA has been repealed to the extent that it now only governs access to the Health Record of deceased patients and applies only to records created since 1st November 1991. The Act allows access for the patient's personal representative and any person who may have a claim arising out of the patient's death.

There are additional provisions for withholding disclosure:

- The deceased person may have specifically prohibited disclosure.
- The information was provided with the expectation that it would not be disclosed to the applicant.
- If disclosure of the information would cause serious harm to the physical or mental health of any person, in the opinion of the relevant professional.
- If disclosure would identify a third party.

4.8 The Access to Medical Reports Act 1988

This Act allows individuals to see Medical Reports written about them for insurance or employment purposes, written by a doctor or clinician who they normally see in the normal doctor/patient capacity. This right can be exercised before or after the report has been sent.

4.9 The Freedom of Information Act 2000

Under this Act personal data of the applicant is exempt under section 40(1) of the Freedom of Information Act 2000 and these requests will instead be dealt with as Data Protection Act SARs. Personal data of another person is exempt under section 40(2) of the Freedom of Information Act 2000 if disclosure would breach one of the data protection principles.

4.10 The Human Rights Act 1998

Article 8.1 of the Human Rights Act 1998 provides that “everyone has the right to respect for his private and family life, his home and his correspondence”. This is however, a qualified right i.e., there are specified grounds upon which it may be legitimate for authorities to infringe or limit those rights and Article 8.2 provides “there shall be no interference by a public authority with the exercise of this right as it is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedom of others”.

4.11 Redaction

This is the act of removing, or otherwise making certain information unavailable. In the instance of a SAR this could include information covering one of the areas below:

- Third Party Information – this does not constitute information received from other organisations, but information relating to other individuals who are not health professionals, i.e. Parent, Spouse, Partner, etc.
- Legal Information – Where legal information has been copied in to an individual’s personal information there is the ability to remove this data
- Harmful Information – Where information, if released, may cause serious harm to the physical or mental health or condition of anyone (and this can include a professional) then it can be withheld.

5. Responsibilities

5.1 The University Hospitals Plymouth NHS Trust Board of Directors

The University Hospitals Plymouth NHS Trust Board of Directors is responsible for ensuring all valid SARs are managed in accordance with the GDPR 2018. The Trust will ensure that a Senior Manager is responsible for the management of all SARs in accordance with the GDPR and this policy.

5.2 Senior Information Risk Owner (SIRO)

This role is undertaken by the Director of Corporate Business who will have executive responsibility for ensuring compliance with the requirements of the GDPR via the Caldicott and Information Governance Assurance Committee (CIGAC). The SIRO is supported by Information Asset Owners (IAOs) from across the Trust. The role of an IAO is to understand what information is held in their area and ensure that Information Asset Administrators (IAAs) can support the Disclosure Team by providing the relevant information for each SAR. Details of how each system provides SAR information should be documented in the relevant System Level Security Policy.

5.3 Caldicott Guardian

The Caldicott Guardian will ensure compliance with the Caldicott Principles via CIGAC.

5.4 Director of IM&T

The Director of IM&T has delegated operational responsibility to ensure that the organisation's Subject Access Rights processes are in place and fully compliant with the requirements of the GDPR through the Integrated Digital Care Record Group (IDCR). The Director of IM&T will delegate the day to day management of SARs to the Head of Health Records and eNotes Implementation.

5.5 Data Protection Officer

The Data Protection Officer will ensure compliance with GDPR (and the new Data Protection Act in due course) via CIGAC.

5.6 Head of Health Records and eNotes Implementation

The Head of Health Records and eNotes Implementation has delegated managerial responsibility for the day to day management of all SARs in line with the requirements of GDPR and this Policy.

5.7 Disclosure Team

The Disclosure Team, based at the Central Records Library Bush Park, are responsible for processing **all requests** received by the Trust. They are responsible for retrieving information for the requester from the Trust's main patient information systems and from the patient's paper health record. The Disclosure Team will also complete a final check of

any information received from Service Lines prior to release of the information to the requester. Please refer to Appendix 3 for the checklists used by the Disclosure Team.

5.8 **Service Lines**

Service Lines are responsible for responding to any requests from the Disclosure Team within 10 days of receipt. Service Lines should provide all information from their area and any local system for each request received. This information MUST be checked by the Service Line prior to sharing with the Disclosure Team to ensure the information is accurate, complete and does not include any third party or other patient's information. Service Lines should inform the Disclosure Team if they do not hold any records for the patient.

5.9 **Electronic Health Records**

- If the SAR includes a request for information held on other electronic Trust systems then the relevant System Manager is contacted by email to request this information. This information **MUST** be checked by the System Manager prior to sharing with the Disclosure Team to ensure the information is accurate, complete and does not include any third party or other patient's information. The System Manager must provide this information to the Disclosure Team within 10 days of receipt. System Managers should inform the Disclosure Team if they do not hold any records for the patient.
- All Data from systems to which the Disclosure Team have access will be printed and scanned.

5.10 **All managers will ensure their staff**:

- Are aware of this policy and related procedures.
- Know how to deal with requests for personal/patient identifiable information.
- Know how to access and store personal/patient identifiable information.

5.11 **All staff will be expected to**:

- Comply with this policy and all related procedures.
- Ensure that all personal/patient identifiable information is accurate, relevant, up to date and used correctly whether stored electronically or on paper.
- Ensure that all personal/patient identifiable information is kept secure at all times.
- Complete annual Information Governance Training.

6. Procedure to Follow

6.1 All requests for access to records (whether they are health records or personnel/employee records) should be made in writing (emails are accepted). A completed SAR form (Appendix 4) must be completed where necessary. Requests must be sent to:

Disclosure Team
University Hospitals Plymouth NHS Trust
Central Records Library
Unit 4, Bush Park
Estover

Plymouth
PL6 7RG

Or via email: plh-tr.DislosureTeam@nhs.net

- Where an individual is unable to make a written request it is the view of the Department of Health that to serve the interest of the patient, it can be made verbally with the details recorded on the individual's file. Should they wish to view the record, provision will be made by the Disclosure Team Supervisor for this to happen under supervision.

6.2 The requester should provide enough proof of identity to satisfy the Disclosure Team of their identity and to allow them to locate the information as required. If this information is not included in the original request, proof will be requested as required.

6.3 Upon receipt of a request for information the Disclosure Team will follow the SARs Standard Operating Procedure (SOP).

6.4 A Subject Access Request (SAR) can be received by anyone within the Trust. If you receive a SAR this MUST be sent to the Disclosure Team immediately for them to action. All SARs MUST be completed within 30 calendar days of receipt; otherwise the Trust will breach the target.

6.5 For further information please refer to the Disclosure Team Page on StaffNET.

6.6 Requests from the Police

Requests received from the police for medical statements should be directed to the Disclosure Team, in order that they can identify the clinician to provide the statement. The Disclosure Team will forward the request, relevant police documentation and patient's consent to the clinician, for this to be actioned and provide the police officer with the relevant contact details. The clinician will provide the statement directly to the police, using the contact details provided on the original request.

All requests for disclosure of health records should be directed to the Disclosure Team to be actioned.

In cases of the Police needing urgent access to information or if there is no consent from the patient to release the information then the request to disclose information must be provided on Police Personal Data Request Form 277. This will be considered by the Emergency Planning and Liaison Officer (EPLO) or On-call Manager in order that the request can be risk assessed and actioned, as appropriate.

6.7 Request to view CCTV images

Requests for CCTV images should be made in writing to:

Assistant Operations Manager or Facilities and Environmental Services Manager
Facilities Department
First Floor, Site Services Building
Derriford Hospital
Derriford Rd
Plymouth
PL6 8DH

Urgent requests from the police for CCTV images to be produced, in support of a high risk live investigation/searches can be produced and disclosed by Indigo Security to the police.

7. Overall Responsibility for the Document

The Head of Health Records and eNotes Implementation has overall responsibility for the development review and implementation of this Policy.

8. Consultation and Ratification

The design and process of review and revision of this policy will comply with The Development and Management of Formal Documents.

The review period for this document is set as one year from the date it was last ratified, or earlier if developments within or external to the Trust indicate the need for a significant revision to the procedures described.

This document will be reviewed by the CIGAC and IDCR and ratified by the SIRO.

Non-significant amendments to this document may be made, under delegated authority from the Head of Health Records and eNotes Implementation, by the nominated owner. These must be ratified by the SIRO.

Significant reviews and revisions to this document will include a consultation with named groups, or grades across the Trust. For non-significant amendments, informal consultation will be restricted to named groups, or grades who are directly affected by the proposed changes.

9. Dissemination and Implementation

Following approval and ratification, this policy will be published in the Trust's formal documents library and all staff will be notified through the Trust's normal notification process, currently the 'Vital Signs' electronic newsletter.

Document control arrangements will be in accordance with The Development and Management of Formal Documents.

The document owner will be responsible for agreeing the training requirements associated with the newly ratified document with the Head of Health Records and eNotes Implementation and for working with the Trust's training function, if required, to arrange for the required training to be delivered.

10. Monitoring Compliance and Effectiveness

Compliance with the 30 day target will be reviewed on a monthly basis. The reasons for any non-compliance will be escalated to the Central Records Library Manager by the Disclosure Team Supervisor. If the reasons for non-compliance sit within the Service

Lines and/or with System Managers then this will be escalated to the Central Records Library Manager by the Disclosure Team Supervisor for further escalation within the relevant Care Group areas.

There is a risk on Datix (ID 6137) for non-compliance with the 30 day calendar rule for SARs. Regular reports detailing SARs compliance and performance will be presented to CIGAC. The Central Records Library Manager will present the report and respond to any queries or questions that are raised.

11. References and Associated Documentation

- UHPNT SAR Standard Operating Procedure (SOP)
- The Data Protection Act 2018
- The General Data Protection Regulation (GDPR) from the 25th May 2018
- Access to Health Records Act 1990 (for Deceased patients)
- The Access to Medical Reports Act 1988
- The Freedom of Information Act 2000
- Confidentiality: NHS Code of Practice
- Information Commissioners Office Codes of Practice
- Records Management Code of Practice for Health and Social Care 2016

Dissemination Plan and Review Checklist | Appendix 1

Dissemination Plan	
Document Title	Subject Access Request (SAR) Policy
Date Finalised	June 2018
Previous Documents	
Action to retrieve old copies	Initial document

Dissemination Plan

Recipient(s)	When	How	Responsibility
All Trust staff	August 2018	Vital Signs	Document Control

Review Checklist		
Title	Is the title clear and unambiguous?	Yes
	Is it clear whether the document is a policy, procedure, protocol, framework, APN or SOP?	Yes
	Does the style & format comply?	Yes
Rationale	Are reasons for development of the document stated?	Yes
Development Process	Is the method described in brief?	Yes
	Are people involved in the development identified?	Yes
	Has a reasonable attempt has been made to ensure relevant expertise has been used?	Yes
	Is there evidence of consultation with stakeholders and users?	Yes
Content	Is the objective of the document clear?	Yes
	Is the target population clear and unambiguous?	Yes
	Are the intended outcomes described?	Yes
	Are the statements clear and unambiguous?	Yes

Evidence Base	Is the type of evidence to support the document identified explicitly?	Yes
	Are key references cited and in full?	Yes
	Are supporting documents referenced?	Yes
Approval	Does the document identify which committee/group will review it?	Yes
	If appropriate have the joint Human Resources/staff side committee (or equivalent) approved the document?	N/A
	Does the document identify which Executive Director will ratify it?	Yes
Dissemination & Implementation	Is there an outline/plan to identify how this will be done?	Yes
	Does the plan include the necessary training/support to ensure compliance?	Yes
Document Control	Does the document identify where it will be held?	Yes
	Have archiving arrangements for superseded documents been addressed?	Yes
Monitoring Compliance & Effectiveness	Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	Yes
	Is there a plan to review or audit compliance with the document?	Yes
Review Date	Is the review date identified?	Yes
	Is the frequency of review identified? If so is it acceptable?	Yes
Overall Responsibility	Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the document?	Yes

Equalities and Human Rights Impact Assessment	Appendix 2

Core Information	
Date	August 2018
Title	Subject Access Request (SAR) Policy
What are the aims, objectives & projected outcomes?	To outline how access requests for personal information will be managed by the Trust in accordance with the General Data Protection Regulation (GDPR) (EU) 2016/679 (from 25th May 2018), the Access to Health Records Act 1990 (for deceased patients) and the Access to Medical Reports Act 1988.

Scope of the assessment
This policy highlights the following: What action Trust staff should take upon receipt of a SAR. Who is responsible for completing SARs. How the Trust will action SARs. How the Trust will protect information when being disclosed.

Collecting data	
Race	This is mitigated as the policy can be made available in alternative languages.
Religion	This policy has no impact in this area.
Disability	This is mitigated as the policy can be made available in alternative formats.
Sex	This policy has no impact in this area.
Gender Identity	This policy has no impact in this area.
Sexual Orientation	This policy has no impact in this area.
Age	This policy has no impact in this area.
Socio-Economic	This policy has no impact in this area.
Human Rights	This policy has no impact in this area.
What are the overall trends/patterns in the above data?	There are no trends/patterns in this data.

Specific issues and data gaps that may need to be addressed through consultation or further research	Trust wide documents can be made available in a number of different formats and languages if requested.

Involving and consulting stakeholders	
Internal involvement and consultation	
External involvement and consultation	
Impact Assessment	
Overall assessment and analysis of the evidence	

Action Plan

Action	Owner	Risks	Completion Date	Progress update

DISCLOSURE CHECKLIST

HANDLER'S NAME: ----------

PATIENT: ----------

DOB: ----------

HOSP NO: ----------

SOLICITORS NAME: ----------

DATE OF REQUEST: ----------

DATE OF DISCLOSURE: ----------

CHECKED BY: ----------

RECORDS/INFORMATION REQUESTED

	Date requested	Date received	Notes
HEALTH RECORDS/UNITY PRINTOUT			
RADIOLOGY REPORTS (ALL)			
RADIOLOGY IMAGES			
A&E CARDS – if relevant to the request (Printouts are not acceptable for a potential claim)			
OPHTHALMIC RECORDS – if relevant to the request (could be needed for some Neuro incidents)			
PHYSIOTHERAPY RECORDS – if relevant to the request (Printouts are acceptable for third party requests)			
AUTOMATED RECORDS Histology, Microbiology & IT			

Pathology			
INNOVIAN RECORDS (ICU and Cardiac ICU) – If relevant to the request			
MEDICAL PHOTOGRAPHS – if relevant to the request			
INFLOFLEX – if relevant to the request (Rheumatology, Colorectal and Cancer Services are currently using this system)			
iPM printout (only provided if all records are requested)			
Other			
MISSING RECORDS Details of all searches made.			
For Potential Claims:			
COMPLAINTS FILE No (no redaction needed):			Censor checked by:
INCIDENT REPORT No (must provide the Rich Client Risk Manager Version):			Censor checked by:

ROOT CAUSE ANALYIS – FINAL VERSION (must provide the Rich Client Risk Manager Version):			Censor checked by:
POLICIES/PROTOCOLS – If exact policy specified by Solicitor. Name of Policy:			

For Potential Claims please scan a completed copy of this checklist and email to: plh-tr.legaldepartment@nhs.uk

SAR Request Form | Appendix 4

Subject Access Request Form

1) Personal Information about the Data Subject:			
Surname:			
Forename(s):			
Title:			
Date of birth: Date of death (if applicable):		NHS/Hospital/Payroll Number (if known):	
Current address:			
Telephone number:			
If name and/or address was different from the above during the period(s) to which the application relates, please give details below:			
Previous surname(s):		Previous forename(s):	
Previous address:			
For office use only			
Handler's name:	Disclosure date:	Patient name and d.o.b checked:	Hospital number:

2) Details of records being accessed:

Please provide as much information as possible of the dates/episode (s) for which you require access to. If you are requesting all information then please state this.

Please note that we are only able to disclose records and radiology images in respect of treatment received whilst under the care of University Hospitals Plymouth NHS Trust and therefore you will have to approach each individual Trust if you also had treatment elsewhere.

Consultant/speciality (if known):

Date(s) (if known):

Clinic/Ward attended (if known):

Other records excluding health records:

Accessing/disclosure option:

Under the EU General Data Protection Regulation (GDPR), from the 25th May 2018, there will be no charge for these requests except in specific circumstances, such as if the requests are manifestly unfounded, excessive or if it is a request for further copies.

I would like photocopies of the records pertaining to the dates stated above **yes/no**

I would like copy radiology images relating to the dates stated above **yes/no**

I would like to attend the Disclosure Team to view the original information **yes/no**

3) Consent

Please confirm whether you are:

Data subject, applying for copies of your own records (go straight to section 4) ☐

Person with parental responsibility for data subject ☐

Representative of the data subject ☐

If you are either the person with parental responsibility or representative of the data subject (evidence must be provided) then please complete the following:

Surname:

Forename(s):
Title:
Address:
Telephone number:
*Please note that if you are applying for access to information concerning another adult patient who is not deceased, then that person **must** provide their consent below:* I (data subject full name)…….. hereby authorise Plymouth Hospitals NHS Trust to release details of information as requested overleaf to …….to whom I have given consent to act on my behalf.
Signature:
Date:
4) Proof of Identification
Please provide **a copy** of one of the following documents as proof of identification: Current valid Passport (any country) Current Driving Licence – Full or provisional HM Forces ID Card EU National ID Card Mortgage Statement Bank/Building Society Statement Council Tax Statement Utility Bill – e.g. landline telephone, water, electric, gas. **(Not Mobile Telephone)** Benefit Statement - e.g. Child Allowance, Pension A document from Central/Local Government/Government Agency/Local Authority giving entitlement – e.g. from the Department for Work and Pensions, the Employment Service, Customs & Revenue, Job Centre, Job Centre Plus, Social Security Letter from Head Teacher or College Principal Letter from Nursing/Residential home

5) Declaration by applicant *WARNING – You are advised that making untrue statements in order to obtain access to personal information, to which you are not entitled, is a criminal offence.*
I declare to the best of my knowledge and belief that the information given on this form is correct.
Signature:
Date: