MEDICAL SERVICES

PROVIDED ON BEHALF OF THE DEPARTMENT FOR WORK AND PENSIONS

Medical Services

The Data Protection Act

MED-TDPA01

Version: 3 (final)
22 August 2012

Document Control

Version	Date	Comment
3 (final)	22 Aug 2012	Immediate re-review to make additions requested by DWP re: from ownership
2 Final	18 July 2012	General Review
1 Final	14 February 2011	Approved by CMMS

Superseded Documents

Changes since last version

Outstanding issues and omissions

Updates to Standards incorporated

Issue

Author: Process Design Team

Owner and approver: The Process Design Team Manager Date: 22 Aug 2012

Contents

1.	**About this document**	**5**
1.1	Purpose	5
1.2	Applicability	5
1.3	Owner	5
1.4	References	5
2.	**Introduction**	**6**
2.1	The Data Protection Act 1998	6
2.2	The Principles of the Data Protection Act	6
2.3	Subject Access Requests	6
3.	**Definition**	**7**
3.1	Data Subject	7
3.2	Data Controller	7
3.3	Data Processor	7
3.4	Data Protection officer	7
3.5	Definition of ‘Processing’	7
4.	**Data Processing**	**8**
4.1	Use of Data	8
4.1.1	Personal responsibilities for Processing Data	8
4.2	Consent for Data Use	9
4.2.1	Personnel	9
4.2.2	Security and IT	9
4.3	Retention	10
4.4	The Data Protection System	10
4.4.1	Monitoring Policy	10
4.4.2	Register of Access Requests	10
4.4.3	Requests for copies of documentation	10
5.	**Process for Dealing with a Subject Access Request**	**12**
5.1	Generic Process	12
5.1.1	Target Dates	12

5.2 Claimant Requests Data 12
5.2.1 Process 13
5.2.2 What happens if the request is received by the Data Processor 14
5.3 Harmful Information 14
5.4 Subject Access Requests made by Personnel working on the Medical Services Contract 15
5.5 Subject Access Requests made in respect of Atos Healthcare's occupational health DWP contract 15
6. Third Party Data 16
6.1.1 General 16
6.1.2 Other Data 16
Appendix A - The Principles of the Data Protection Act 17
Appendix B - Process for Dealing with Subject Access Requests 20
Appendix C - Medical Services Data Protection Officer 21
Appendix D - DPT 1 22
Observation form 23

1. About this document

1.1 Purpose

The purpose of this document is to ensure that all members of Atos Healthcare (AH) are aware of the Data Protection Act (DPA). The guidance will provide understanding on the processes and procedures to be followed to ensure compliance with the act and also during the process of a request from an individual for copies of their personal data.

1.2 Applicability

All Atos Healthcare Staff, Atos staff, contractors and third parties working on any DWP Medical Services contracts in place.

1.3 Owner

The Process Design Team Manager owns this document.

The owner is responsible for approval of this document and all related feedback should be addressed to them.

1.4 References

1. Document Processing and Retention Handbook (MED-DPRH01)

2. Introduction

2.1 The Data Protection Act 1998

The Data Protection Act became law on 1 March 2000. A wide ranging review of personal data and their use throughout Atos Healthcare (AH) was undertaken at the time. The objective was to ensure that all operational procedures were, or would be made, compliant with the Data Protection Act 1998 (DPA).

In particular, the DPA contains eight Principles which define how personal information should be treated and gives individuals certain rights.

Atos Healthcare (AH), as part of Atos IT Services UK Limited (Atos), is acting for Medical Services contracts in the role of Data Processor and the customer is the Data Controller. However, AH is not always the Data Processor: depending on the situation AH can also be the Data Controller e.g. with regard to employee records.

2.2 The Principles of the Data Protection Act

Any organisation that controls the processing of personal data must comply with the DPA. In this context 'process' means any action associated with data, including for example, the collection of data.

The DPA contains 8 principles which define the key requirements of data protection. These are listed at Appendix A.

The Company Data Privacy Policy provided senior management commitment to comply with all the requirements of the Act. This can be obtained from the UKI Intranet, reference: SEC-POL050.

2.3 Subject Access Requests

This guide will provide further in sight into a specific process, dealing with a Subject Access Request (a request from an individual for a copy of their own personal information). It explains how to deal with these requests, ensuring they comply with the DPA. It is important that this guide be read in conjunction with the Document Processing and Retention Handbook (MED-DPRH01).

3. Definition

Below are the definitions of terms used in relation to the process of complying with the DPA.

3.1 Data Subject

The Data Subject is a living individual who is the subject of personal data.

3.2 Data Controller

The Data Controller is the organisation or person who determines the purposes for which information is processed and the manner in which this is done. The Data Controller may be a government department (such as the DWP) or a company (such as Atos).

3.3 Data Processor

A Data Processor is an organisation or person that processes data on behalf of a data controller. For example, in respect of Medical Services, AH acts as a data processor on behalf of the DWP.

3.4 Data Protection officer

The role of the Data Protection Officer for Medical Services is to ensure that fair and lawful processing is applied and that all data subject access requests are processed correctly.

The Data Protection Officer will liaise, as necessary, with the Atos UK Data Protection Manager.

3.5 Definition of 'Processing'

In the DPA, 'processing' is defined in such a way that it encompasses every action that could be performed on data. This includes data collection, data storage, data processing (in the conventional sense), data transmission, data output, data disclosure, data distribution and data archiving and deletion. All these actions which an organisation will undertake must 'line up' with the stated purpose for processing.

4. Data Processing

Personal data requested by a Data Subject has to be released in full unless specifically exempted under the Act. This includes any notes that may be "off the record" or marked "confidential" but do not fall under the definition of Harmful Medical Information. A Data Subject may ask for historical information which, if in the possession of the Data Controller/Processor, has to be released.

Exemptions relating to third party data are dealt with in section 6. There are other exemptions, for example data that is subject to legal professional privilege. If in doubt, guidance should be sought from the Data Protection Officer.

4.1 Use of Data

Personal data must be processed fairly and lawfully. In particular, the processing must have a legal justification – as defined in the Act – for taking place; and more stringent rules apply to data of a more sensitive nature e.g. health related data or the indication in a record of ethnic origin. There must be a purpose for processing, for example, storage is processing.

Where AH is acting as the Data Processor, the legal justification for processing is given by the contract with the customer and not by the Act itself. It will be for the customer to show compliance with all eight Principles of the Act and they cannot be absolved of responsibility for this. However, they may and should specify certain contractual obligations associated with the terms of the Act.

In cases where it is agreed that AH (strictly speaking Atos as AH is a branch of this company) is acting as the Data Controller, the legal justification for processing will need to be identified and documented for the purposes of notification under the Data Protection Act. The Atos UK Data Protection Manager is responsible for all AH notifications.

4.1.1 Personal responsibilities for Processing Data

- The quality of output must be considered and personal data should be adequate, relevant and not excessive, e.g. information that is not needed should not be kept
- Hand written notes must only contain factual information and keep it as brief as possible, **do not add sarcastic or any other personal comments**
- Only hold information for as long as it is required for action to be taken and as long as there is a legal or business need for its retention. Data must not be kept once the purpose for processing has lapsed.
- Information should be accurate and kept up to date (see 4.4 for further details on retention).
- 'Post-It' notes should never be filed – destroy them when the message has been

actioned.

- E-mails should only refer to ONE subject/person at a time and should not be added to a long string of replies about other matters or individuals (this would not apply to a straight forward list of names)

- Emails should be deleted as soon as is practicable – if they are retained they must be made available on a data subject request. Note: it should not be necessary to have any reference to a claimant made in emails. However, if it is appropriate to do so, this should be printed and placed into the relevant file.

- It is essential that nothing derogatory about an individual is ever enclosed in emails.

4.2 Consent for Data Use

4.2.1 Personnel

AH Personnel are responsible for compliance with the DPA in respect of employee personal data.

4.2.2 Security and IT

The DPA sets out requirements and good practice guidelines for handling personal information that has been computer-processed.

The Act states that personal data must only be used for the purposes for which it has been collected and the purposes must have been registered with the Information Commissioner.

- **Access** – Staff may only access the records of those claimants they have to process in the course of their work (this applies to both computer and hard copy records). They have no right to access claimant records for any other reason and deliberately or carelessly doing so is a disciplinary offence.

- **Quality –** Personal data must be accurate, up-to-date and relevant. If in the course of their duties staff find data about a claimant that is obviously wrong for any reason, they should inform their Line Manager who will arrange for the record to be reviewed.

- **Security –** Security measures must be in place to protect personal data from unauthorised access or disclosure. It is vital to follow the security policies and procedures to ensure the confidentiality.

Detailed procedures relating to Security can be found by accessing the Atos Healthcare Security area on Livelink.

4.3 Retention

Ensure information or data is not held beyond the retention periods given in the Document Processing and Retention Handbook (MED-DPRH01).

- Personal data should not be kept for longer than is necessary for the purpose(s) of processing

- Information should be accurate and kept up to date. Reasonable effort must be made to ensure that data is recorded accurately. Once recorded, ensure that the data is kept up to date for changes in the personal circumstances of the individual or other business related data, which may be recorded.

- Duplication of data – Information should be held in as few places and ways as possible e.g. avoid running clerical and IT systems for the same data. Business efficiency can be gained by minimising data duplication where possible. The more data is duplicated and used operationally, either electronically or manually, the more likely that useable data is not properly updated at the right time and becomes out of date. **The duplication of healthcare personal data must be carefully controlled.**

- Data collected by OHCSS on candidates who are subsequently rejected for employment should be deleted from the electronic file and paper records and forms should be shredded.

4.4 The Data Protection System

The Data Protection System will consist of all the mechanisms and procedures put in place to ensure compliance with the Act. This will consist mainly of policies and procedures but will also include all the security protection.

4.4.1 Monitoring Policy

Monitoring of internet use and investigation of email use may be undertaken in line with the Atos Computer Usage Policy (UKM-HR-0012). Members of staff need to consider all their working paper records and any electronic data held on Atos Healthcare systems against the list of personal responsibilities in section 4.1.1.

4.4.2 Register of Access Requests

The Medical Services Data Protection Officer (DPO) will maintain a register of requests and will update it with information on the dates received and cleared, together with the date of the subject access request and the details of the requesting individual.

4.4.3 Requests for copies of documentation

The ESA 85 or any subsequent medical reports for any other medical referrals are

not the property of Atos Healthcare and any such requests must be forwarded to DWP Service Integration Team.

5. Process for Dealing with a Subject Access Request

5.1 Generic Process

This generic process refers to Subject Access Request's made in respect of the Medical Services contract, provided on behalf of the Department for Work and Pensions.

Please see section 3 for definitions and Appendix B -for the flowchart on this process.

When a Data Subject requires personal data held on themselves, they should issue a written request to the appropriate Data Controller. When the request is received by the Data Controller, they will examine the request. The Data Controller will then decide whether the request is valid, if it is not, they will return the request to the Data Subject with an explanation as to the reason for rejection. There are a few instances were a SAR could be refused, for example; if the Data Subject had not made their request in writing; or if a request was made by a third party, on behalf of the Data Subject. In these cases written consent must be sought from the Data Subject. If, however, this is accepted and there is a third party involved in holding information on the Data Subject the Controller will issue the request to the Data Processor. When the request is received by the Data Processor it should be forwarded to the Data Protection Officer. When all the data has been collected the Data Protection Officer will reply with any observations to the Data Controller who will then reply to the Subject Access Request with any relevant explanation about data that may have been withheld.

5.1.1 Target Dates

There is a 40-day period that applies to the Data Controller, this starts from the date the request is received by the Controller and ends when the final reply is sent to the Data Subject. Where the DWP is the Data Controller and AH, the Processor, there is a 10 working day target that applies to Medical Services. The Subject Access Request (SAR) will be sent, by e-mail, from CMMS to AH containing name, address and NINO details. The 10-day target starts when the e-mailed request is received by Medical Services and ends when Medical Services notify CMMS, by e-mail and/or any hard copy information has been forwarded to CMMS.

5.2 Claimant Requests Data

From 23 October 2001 all documents, those completed by Health Care Professionals (HCPs) and all information held on either systems or clerically, that concern a claimant such as responses to complaints, have to be released in full if requested. This also includes those that may be "off the record" or marked "confidential" but do not fall under the definition of Harmful Medical Information. A

Data Subject can make a Subject Access Request to any organisation (Atos, DWP or any other organisation) that holds personal information about themselves (Data Subject). However, the data requested can only be shown to the claimant if the material is related directly to that particular person, known as the 'data subject'.

The claimant should issue a written request to the appropriate Data Controller, they may also be charged for information requested and provided to them. However, it has been agreed that where Atos is the Data Controller, there will not be a charge. The DWP will also not charge for information provided.

Please note: The ESA 85 or any subsequent medical reports for any other medical referrals are not the property of Atos Healthcare and any such requests must be forwarded to DWP Service Integration Team.

5.2.1 Process

The DWP refers claimants to AH Medical Services for medical examination and assessment in support of their claim to benefit. DWP is the Data Controller for this data. When information is required by the claimant they should issue their request to the DWP (the Data Controller). The DWP will examine the request to ensure that it is complete. This will include proof of identity and an acceptable description of the data required. When a complete request is received by DWP, the date of receipt is the first day of a 40 day period (calendar days, **not** working days) for a reply to be issued to the claimant, including the time it will take for DWP to send the request to Medical Services and receive the response.

In this instance Medical Services is the 'Data Processor'. Once the request has been received in Medical Services, it should be forwarded to the Medical Services Data Protection Officer (details of the current Medical Services DPO can be found at Appendix C -). Subject access requests from the Disability and Carers Service (DCS) will be referred to Medical Services via CMMS. Jobcentre Plus (JCP) Benefit Centres (BC) will refer requests by written letter.

5.2.1.1 Medical Services Data protection Officer Action

When the request is received by the DPO for Medical Services, the case will be registered on a log; the DPO will also check for any complaints received by/on behalf of the data subject. If this **is** the case, the DPO will contact the relevant Customer Relations Manager and request copies of all:

- complaints file documents,
- other correspondence
- any screen prints relating to the individual

This information should be provided in hard copy.

The Medical Services DPO will then:

- update the comments section of the register

- review the contents to ensure it is relevant to the request
- identify any potentially sensitive issues

Once all investigations have been made and all of the above action has been taken, the Medical Services DPO will:

- reply to the Data Controller, with any observations. The Medical Services DPO will send the papers, with a cover note, explaining any concerns, to the Data Controller.
- where there is information relating specifically to a third party e.g. a HCP home address, the Medical Services DPO will remove this information prior to issuing to the DWP Data Controller
- keep a copy of those documents released to the Data Controller (in case of loss in the post, dispute of information provided etc.)
- update the register

The reply must be provided to CMMS within 10 working days of receiving the request (see 5.1.1).

The Data Controller has the final decision on what is to be disclosed to the Data Subject.

5.2.2 What happens if the request is received by the Data Processor

If a request from the Data Subject is received by Medical Services directly, the request must be forwarded **immediately** to the appropriate Data Controller and a letter (DPT 1) issued to the claimant explaining what has happened. An example of this letter is shown at Appendix D. The 40-day period will not start until the request has been received by DWP Data Controller.

5.3 Harmful Information

An exemption was added to the subject access provisions in the DPA in respect of data relating to the mental/physical health or condition of the data subject. This exemption covers data that is likely to cause serious harm to the physical/mental health or condition of the data subject.

The arrangements that are in place to deal with harmful data are there to make sure that such data is clearly identified and that, where appropriate, a HCP will verify whether this restriction is still in place. If so, the data should not be disclosed as part of a data subject access request. This would include not telling the subject that certain data had been omitted – if something is exempt then it should be ignored.

Where harmful information may be contained within an AH form (such as an ESA85) and a SAR is received from the subject, regarding information held within their file, the DWP must refer the file to Medical Services to ask if the information can be

released to the subject.

When received at Medical Services, these cases will be referred to the Medical Adviser, for a decision on whether the information should be disclosed to the individual.

5.4 Subject Access Requests made by Personnel working on the Medical Services Contract

All employees have the right over their own personal data held by AH. Any requests for personnel data must be passed to AH HR .

Atos is the Data Controller for data requested by an Atos employee, on themselves.

It is important that you ensure your own personal records are accurate and up to date.

5.5 Subject Access Requests made in respect of Atos Healthcare's occupational health DWP contract

Medical Services provide occupational health services (OHCSS) to the DWP and a number of other customers. Atos is the Data Controller in respect of medical records that are obtained in the course of delivering these services. All such Subject Access Requests should be forwarded to:

Atos Healthcare, Unit 2, Hayland Street, Meadow Court, Sheffield, S9 1BY, or: xxxx@xxxxxxxxxxxxx.xxm or by internal address book ""Medical in Confidence Requests".

6. Third Party Data

6.1.1 General

Care must be taken, when responding to a subject access request, not to wrongly disclose information about other individuals (third parties). This would clearly be contrary to the idea of protecting personal data.

6.1.2 Other Data

In some situations there may not be enough information, either in the record or otherwise available to the data subject, for the other individual to be identified. In other cases it may be possible to change references to them in a way that protects their identity e.g. by referring to them as "X". However, the latter only makes sense if it is right that they should be anonymous and if just making this simple change actually means that they cannot be identified either directly or from other information available to the data subject.

Otherwise, if the other individual has consented to disclosure then this would normally be acceptable.

Otherwise it is for the Data Controller to decide whether it is right, in the circumstances, to disclose this information. These cases should be submitted to the DPO for a decision. The DPO will take into account:

(a) any duty of confidentiality owed to the other individual;

(b) any steps taken by the data controller with a view to seeking the consent of the other individual and whether any consent has been obtained;

(c) whether the other individual is capable of giving consent, and;

(d) any express refusal of consent by the other individual.

In cases where consent by the other individual has been given for disclosure then normally the decision would be made to disclose. But in all cases the Data Protection Officer will seek to balance the right of the other individual to privacy against the right of the data subject to disclosure.

Appendix A - The Principles of the Data Protection Act

Principle 1

Personal data shall be processed fairly and lawfully, and only if one of a number of conditions is met (there is an additional, more restricted, list of acceptable conditions for processing sensitive data such as health data).

Where AH is acting as the Data Processor, the legal justification for processing is given by the contract with the claimant and not by the Act itself. In this situation it is Atos Healthcare's responsibility to process the data only in accordance with the customer's instructions and to ensure that it is protected against unauthorised use or disclosure.

In cases where it is agreed that AH (strictly speaking Atos) is acting as the Data Controller, then compliance with the DPA is our direct responsibility.

When Atos processes personal data on its own behalf, then it needs to meet the condition for fair processing. When it is acting as a data processor, it is the customer's responsibility to comply with this principle. Atos' justification is that it has a contract with the customer.

Principle 2

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

DWP tell the Information Commissioner, amongst other things, why DWP collects personal information, who we share it with and whether we transfer any personal information overseas. These details are used by the Commissioner to make an entry describing the process in a register which is available to the public for inspection.

DWP also have policy and guidance in place which sets out to staff how personal data is collected and used within the Department. Data must not be used for unlawful or unspecified purposes.

Principle 3

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

If it is considered that any data item is irrelevant or excessive to the purpose, the

matter should be reported to AH Senior Management. If it is considered that the purpose is not properly satisfied without the use of some other, missing data this too should be highlighted.

To meet this requirement DWP ensures we only collect and record personal information that is necessary to meet our business needs, nothing more. The information we record must be based on fact and, where opinion is recorded, it must be relevant.

Principle 4

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

Data should be obtained and processed in a manner that promotes accuracy and ensures that it is kept up to date where required.

Principle 5

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

Refer to Document Processing and Retention Handbook (MED-DPRH01).

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under the DPA.

Individuals have a right to have access to their personal data held by DWP or Atos Healthcare. There are procedures in place to handle subject access requests within 40 calendar days. See Subject Access Procedures

Individuals also have a right to the following:-

a) right to prevent processing likely to cause damage or distress;

b) right to prevent processing for the purposes of direct marketing;

c) rights in relation to automated decision taking;

d) right to take action for compensation if the individual suffers damage by any contravention of the Act by the data controller;

e) right to take action to rectify, block, erase or destroy inaccurate data

Principle 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. In particular, if processing is outsourced to a data processor, there must be a written contract that obliges the data processor to take appropriate security measures.

Security measures must be regularly reviewed. All members of staff must handle personal data carefully, securely and in accordance with company policy.

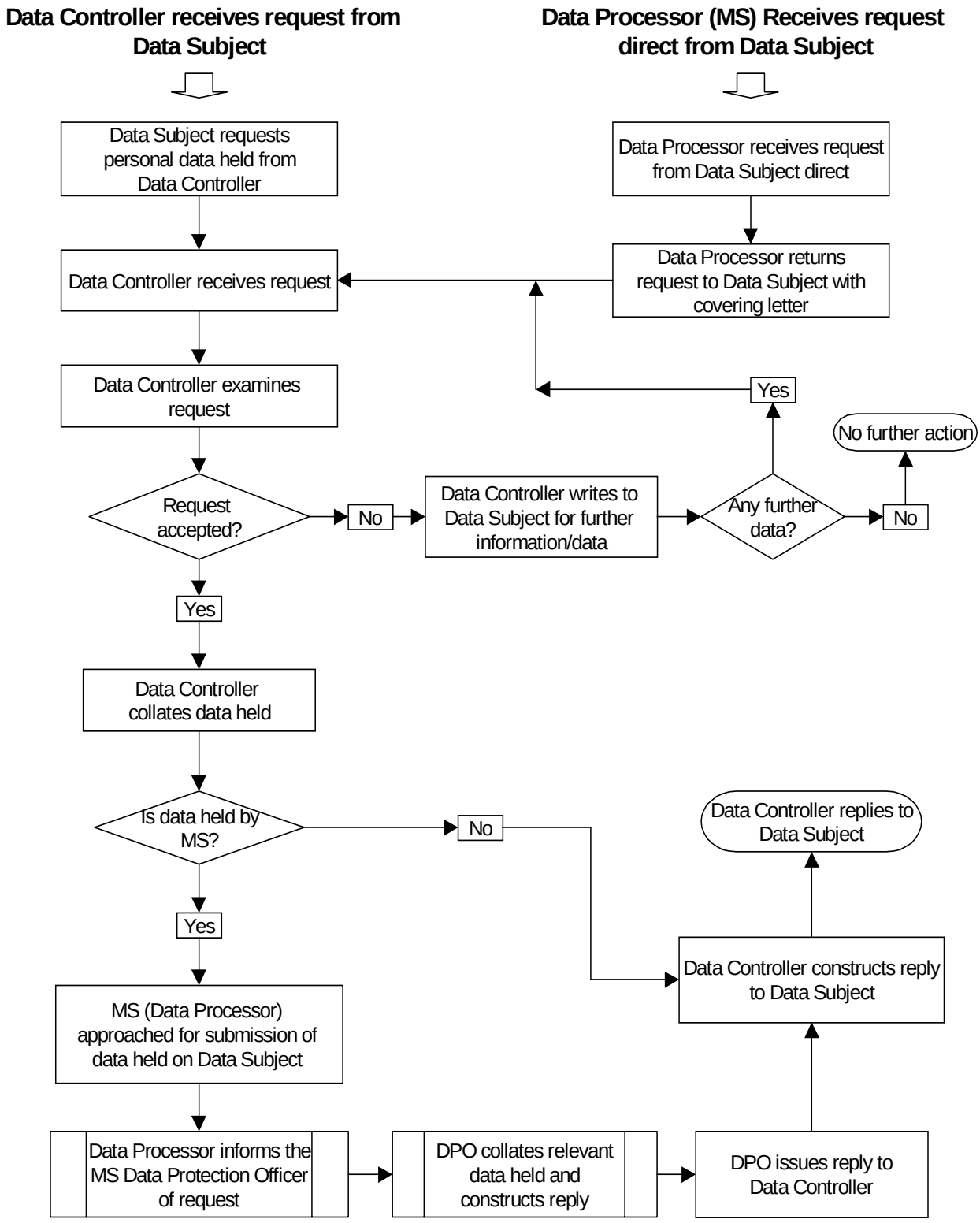
Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA), 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.

AH currently operates only within the boundaries of the UK.

[Note the EEA comprises the EU countries plus Liechtenstein, Norway and Iceland.]

Appendix B - Process for Dealing with Subject Access Requests



Appendix C - Medical Services Data Protection Officer

The Medical Services Data Protection Officer is:

Name Redacted
Wing G, Block 1
Government Buildings
Otley Road
Leeds
LS16 5PU

Tel: Number Redacted

Mobile: Number Redacted

Fax: Number Redacted

Appendix D - DPT 1

MEDICAL SERVICES

PROVIDED ON BEHALF OF THE DEPARTMENT FOR WORK AND PENSIONS

NAME & ADDRESS OF SENDER

Tel:
Fax:

NAME & ADDRESS

DATE:

Dear Mr/Mrs/Miss _____

Re: Request for personal data

I am writing with reference to your request under the Data Protection Act for personal data held in connection with your benefit claim. This request was stated in your letter dated _____ to _____ on _____.

I have now referred your request to the appropriate Data Controller as defined in the Data Protection Act, who is:

NAME & ADDRESS OF DATA CONTROLLER

Any further communication concerning this request should be made to the Data Controller.

Yours Sincerely

NAME & SECTION

DPT 1 NOV 01

Observation form

Please photocopy this page and use it for any comments and observations on this document, its contents, or layout, or your experience of using it. If you are aware of other standards to which this document should refer, or a better standard, you are requested to indicate this on the form. Your comments will be taken into account at the next scheduled review.

Name of sender: _____ Date:_____

Location and telephone number:_____

Please return this form to Atos Healthcare, Process Design Team. Email to R Process Design