**POLICY TITLE:** Data Protection

**Policy Number:** OP02

**Version Number:** 02

**Date of Issue:** 21/11/2014

**Date of Review:** 20/11/2017

**Author:** Tina Walton, Chief Information Officer  
Brian McCallion, Group IT Risk & Compliance Manager

**Ratified by:** Brian McCallion, Group IT Risk & Compliance Manager

**Responsible signatory:** David Watts, Director of Safety

**Outcome:** This policy:
- documents to key delegated officers in connection with Data Protection, including the Caldicott Guardian
- sets out processes around the principles in the Data Protection Act regarding keeping personal information
- deals with Subject Access Requests (SARs)
- provides information sheets for Service Users

**Cross Reference:**  
HR04.8 Protection of Employee Data  
IT02 IT Security  
IT07 Printing, Photocopying, Scanning and Faxing  
OP27 Confidentiality  
OP02.1 Document and Data Retention  
Divisional policies on record keeping

**EQUALITY AND DIVERSITY STATEMENT**  
Priory Group is committed to the fair treatment of all in line with the Equality Act 2010. An equality impact assessment has been completed on this policy to ensure that it can be implemented consistently regardless of any protected characteristics and all will be treated with dignity and respect.

To ensure that this policy is relevant and up to date, comments and suggestions for additions or amendments are sought from users of this document. To contribute towards the process of review, e-mail SQCHelpdesk@priorygroup.com
DATA PROTECTION

CONTENTS

1 INTRODUCTION 2
2 PURPOSE 3
3 DEFINITIONS 3
4 SCOPE 4
5 LEGISLATIVE REQUIREMENTS 4
6 POLICY STATEMENT 4
7 KEY PRINCIPLES 4
8 TRAINING IMPLICATIONS 5
9 GROUP COMPLIANCE 5
10 STAFF RESPONSIBILITIES 6
11 DATA PROTECTION ACT PRINCIPLES IN PRACTICE 6
12 SUBJECT ACCESS REQUESTS 11
13 INDIVIDUAL’S CONSENT 13
14 DISCLOSURE OF PERSONAL INFORMATION 14
15 ANONYMISING INFORMATION 15
16 SHARING INFORMATION BETWEEN ORGANISATIONS 15
17 DATA PROCESSORS 15
18 EXEMPTIONS 17
19 AUDIT 18
20 REFERENCES 18

Appendix 1 – Subject Access Request Flowchart 20
Appendix 2 – Information Sheet for New Staff 22

1 INTRODUCTION

1.1 The DPA sets out the rules and principles in connection with processing personal and sensitive data. It places obligations on a data controller and sets out the rights of data subjects. The Information Commissioner’s Office oversees compliance with the law.

1.2 Priory Group complies with the requirements of the Data Protection Act 1998 (DPA). This policy should be interpreted in conjunction with that Act and Practice Codes published by the Information Commissioner.

1.3 Priory Group companies are registered using their individual company names with the Information Commissioner and the register entry may be inspected at http://ico.org.uk/what_we_cover/register_of_data_controllers. Practices Codes can be viewed at www.informationcommissioner.gov.uk. All health care professionals who have practising privileges and retain personal data about service users must be independently registered as data controllers with the Information Commissioner.

1.4 Priory Group processes personal information for a variety of purposes, including those connected with the employment and engagement of staff, the treatment and care of service users, pupils and residents, management of services and the reduction of risk of harm and the detection, investigation and prevention of crime. Given the core nature of Priory Group’s business, it gives the utmost priority to service users, students and residents confidentiality.

1.5 The responsibility for compliance lies with the Chief Operating Officer, who provides delegated authority to the Group’s Directors (Directors) for their respective business areas. Directors will need to ensure that compliant processes and procedures are in place so that the DPA principles are met.

1.5.1 The Group Legal Council (GLC) has overview of systems to make sure that they are not set up in breach of any of the principles with the data protection legislation.
2 PURPOSE

2.1 To fulfil its legal obligations the Priory Group needs to hold certain types of information about people with whom it deals. These include staff, service users, pupils, residents, and suppliers. This personal information must be managed in lawfully, regardless of how it is collected, recorded, stored and used, whether it’s on paper, on a computer, or recorded on any other type of media. The lawful and correct treatment of personal information is regarded as a vital and important part of maintaining a right to confidence with those with whom the company deals with.

2.2 The Data Protection Act sets out an individual’s right to confidence, which imposes both legal and ethical obligations on Priory Group. These duties apply to all personal information whether held on computer or manually.

2.3 Members of staff are also reminded of their professional obligations of confidence and reference should be made to guidelines from professional bodies, such as the General Medical Council and take account of the Caldicott Committee report on the review of service user identifiable information. (See OP27 Confidentiality).

2.4 Failure to comply with the relevant laws may result in penalties being imposed on Priory Group, and in addition the possibility of staff being investigated by their professional bodies or subject to disciplinary action.

3 DEFINITIONS

3.1 Data Controller – Priory Group is a Data Controller under the definition in the Act, because it determines the purposes for which and the manner in which any personal data is processed, with overall responsibility for compliance lying with the Chief Operating officer (see 1.3.1)

3.2 Data Processor – Any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

3.3 Data Subject – An individual who is the subject of personal data.

3.4 Personal Data – Means data which relates to a living individual who can be identified:
   (a) From the data or
   (b) From the data and other information which is in the possession of or is likely to come into the possession of the data controller
   (c) 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.

3.5 Sensitive Personal Data - Personal data consisting of information as to:
   (a) Racial or ethnic origin
   (b) Political opinions
   (c) Religious beliefs or other beliefs of a similar nature
   (d) Membership of a trade union,
   (e) Physical or mental health or condition
   (f) Sexual life
   (g) Commission or alleged commission by the data subject of any offence, or
   (h) Any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in any such proceedings.

3.6 Recipient – Any person to whom the data are disclosed, including any person to whom they are disclosed in the course of processing data for the data controller.

3.7 Third Party – Any person other than the data subject, the data controller or any data processor authorised to process data for the data controller.
3.8 **Data Protection Advice team** – This team is responsible for overview of Priory Group’s compliance with the DPA and providing day to day guidance to staff on matters relating to the DPA. Within Priory group this will be the Priory Legal Team via LegalMailbox@priorygroup.com.

3.9 **Caldicott Guardian** – This person is responsible within the Priory Group for protecting the confidentiality of service-user health and social care records and enabling appropriate information-sharing. Within the Priory Group this is the Director of Corporate Assurance/Chief Nursing Officer.

3.10 **Senior Information Risk Owner** – This person is responsible for the Priory Group’s information risk policy and risk assessment process ensuring we have a robust incident reporting process for information risks. Within the Priory Group this will be the Chief Information Officer.

3.11 **Service User** - A person receiving healthcare, residential care, support or educational services provided by Priory Group.

4 **SCOPE**

4.1 This policy applies to all permanent, temporary or contracted staff employed by Priory Group on any operational site or in central services, and those working through a practising privileges agreement and to students and volunteers who can access personal information under supervision.

5 **LEGISLATIVE REQUIREMENTS**

5.1 For the purpose of this document, and supporting Priory Group’s aim to ensure that all confidential information will be handled in accordance with:-
(a) Data Protection Act 1998
(b) Access to Health Records Act 1990 (where it still applies)
(c) Common Law Duty of Confidentiality

6 **POLICY STATEMENT**

6.1 Priory Group is committed to complying with the DPA to preserve:
(a) **Confidentiality:** protecting sensitive information from unauthorised disclosure
(b) **Integrity:** safeguarding the accuracy and completeness of information
(c) **Availability:** ensuring that information and vital services are available to authorised users and to ensure that any person identifiable information received, stored, processed or transmitted is done so in a secure environment.

7 **KEY PRINCIPLES**

7.1 The key responsibilities that Priory Group has in relation to the personal data it holds are summarised in the following eight points from the DPA. These must be complied with by all staff that create or are in possession of, or have access to, personal data.

7.2 Staff must ensure personal data is:
(a) Processed fairly and lawfully.
(b) Processed for specified purposes.
(c) Adequate, relevant and not excessive.
(d) Accurate and up-to-date.
(e) Not kept for longer than necessary.
(f) Processed in accordance with the rights of data subjects.
(g) Protected by appropriate security.
(h) Not transferred outside the European Economic Area (EEA) without adequate protection.
(See section 11 for details of putting these principles into practice.)
7.2.1 There are also six information management principles recommended by the Caldicott Review, which should also be considered along with the DPA when dealing with personal data in Health and Social Care settings (see OP27 Confidentiality):
(a) Justifying the purpose of using confidential information.
(b) Only using it when absolutely necessary.
(c) Using the minimum that is required.
(d) Access to personal data being restricted to a need to know basis.
(e) Everyone understanding his or her responsibilities.
(f) Understanding and complying with the law.

7.3 Directors can delegate tasks directly to someone holding a senior management position within their business area. This delegated role will be known as the Data Protection Officer (DPO). On operational sites this person is the School Principal, Hospital Director or registered Home/Service Manager.

7.3.1 Therefore, the DPO has overall responsibility within their sphere of influence for the implementation of this policy and compliance with the DPA. This includes:
(a) Arranging and facilitating training sessions.
(b) Assisting the Data Protection Advice team with Subject Access Requests (see Appendix 1 – Subject Access Request Flowchart)
(c) Acting as an initial point of contact for any data protection issues which may arise within their sphere of responsibility.

7.4 Each Director will ensure any IT system in operation within their business area is used in accordance with IT02 IT Security, and compliantly within the principles of the DPA.

7.5 The IT Department will ensure that any new system complies with the DPA and that all databases that require registration are registered in accordance with the requirements of the DPA.

7.6 The day-to-day responsibilities of enforcing this policy will be devolved to managers, whether on operational sites or in central services. In order to fulfil their roles, the DPO will ensure that regular training is provided to remind staff of their responsibilities and the most effective way of ensuring adequate information security and confidentiality.

8 TRAINING IMPLICATIONS

8.1 Training on the legal and ethical duties of confidentiality owed to service users and staff will take place through the Foundations for Growth, Data Protection and IT Security awareness modules at induction and, following a training needs assessment, this will be supplemented by further training, at a level appropriate for each employee group. IT Security and Data Protection are mandatory FfG modules for all employees, with annual updates.

8.2 Staff on operational sites in particular need to be aware of the following policies:
(a) H11 Consent
(b) OP27 Confidentiality
(c) H62 Healthcare Records
(d) AM62 Residents Records
(e) OP05 Mental Capacity

9 GROUP COMPLIANCE

9.1 To ensure compliance with the DPA Priory Group will:
(a) Observe fully, conditions regarding the fair collection and use of personal data
(b) Meet its obligations to specify the purposes for which personal data is used
(c) Collect and process appropriate personal data, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
(d) Ensure the quality of information used.
(e) Apply strict checks to determine the length of time personal data is held (in accordance with regulatory or contractual obligations).
(f) Ensure that the rights of people about whom information is held, are able to be fully exercised under the Act.

(g) Take appropriate technical and organisational security measures to safeguard personal data.

(h) Ensure that personal data is not transferred abroad without suitable safeguards.

(i) Ensure that personal data shared with other organisations is only shared where appropriate and with full consideration for the 'Data Subjects' rights.

10 STAFF RESPONSIBILITIES

10.1 All members of staff are responsible for ensuring that those who do not have a legitimate need to access personal data, are not able to do so, and to make sure that personal data is not accessible to those who do not have a need to know.

10.1.1 Manual records must not be left in situations where individuals could gain access to the information they contain.

10.2 Staff are reminded that ordinary e-mail communications are not secure unless specific measures are taken, such as using an NHS.net, using approved encryption tools or anonymising data before sending. No personal data is to be transmitted outside the European Economic Area (EEA) without the permission of the Data Protection Advice team and CIO to ensure that any such transfer is undertaken lawfully.

10.3 All members of staff are reminded that accessing personal data without the permission of Priory Group is a criminal offence. This does not mean that staff have to seek specific permission in order to carry out their work but, for example, are not authorised to access personal data about a service user or another staff member unless it is a necessary part of their work or they have been authorised in advance to do so by the COO.

11 DATA PROTECTION ACT PRINCIPLES IN PRACTICE (as set out in section 7)

11.1 Processed fairly and lawfully - A key requirement is to ensure that service users are aware of the purposes for which their data have been obtained, the extent to which it may be shared, the opportunity to make known any objections and who they should contact in the event that they wish to exercise one of their rights under the DPA.

11.1.1 In practice this means staff must:

(a) Have legitimate grounds for collecting and using personal data
(b) Not use data in ways that have unjustified adverse effects on the data subject
(c) Be transparent about the intended use, and give individuals appropriate privacy notices when collecting their personal data (See 'Associated Forms')
(d) Handle people's personal data only in ways they would reasonably expect
(e) Make sure you do not do anything unlawful with the data.

11.1.2 This is known as the 'fair processing of information', this requires staff to:

(a) Be open and honest about your identity;
(b) Tell individuals how you intend to use any personal data you collect about them (unless this is obvious);
(c) Usually handle their personal data only in ways they would expect
(d) Not use their information in ways that unjustifiably have a negative effect on them

NB: The collection of personal data may sometimes be used in a manner that negatively affects an individual without this necessarily being unfair e.g. to impose a fine for breaking the speed limit.

11.1.3 Where personal data is to be shared with other organisations the individual should be told that their information may be shared, so they can choose whether or not to enter into a relationship with the Priory Group.

11.1.4 Unless one of the specific exemptions applies (see section 18), individuals should generally be able to choose whether or not their personal data is disclosed to a third party.
11.1.5 In order for Priory Group to comply with the Data Protection Act principles, all service users must be given the Data Protection Act information leaflet OP Form: 08 or 08C Using and Sharing Information About You and new members of staff will receive OP Form: 11 Data Protection and Service User Information. If any new information is obtained that does not come within the general descriptions contained in those documents, then the service user must be informed of the existence of that data and the purposes for which it is intended to be processed and anything else to enable the processing to be fair.

NB: On request Priory will provide service users and staff copies of OP Form: 08 or 08C Using and Sharing Information About You and OP Form: 11 Data Protection and Service User Information in an accessible format to meet the requirements of Disability Discrimination Act (DDA). Copies can be obtained in large print, audio and Braille by submitting a request to the Priory Marketing Team.

11.2.6 Processed for specified purpose - Personal data must only be obtained specified purposes, and must not be further processed in any manner incompatible with those purposes. In practice this means that staff will:
(a) Be clear from the outset about why it is being collected and what you intend to do with it;
(b) Comply with the Act’s fair processing requirements – including the duty to give the information notice to individuals when collecting their personal data
(d) Ensure that if you wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.

11.2.7 If you wish to use or disclose personal data for a purpose that was not contemplated at the time of collection, you must consider whether it would be unfair because it would be outside what the individual would have reasonably expected or have an unjustified adverse effect on them. In practice, you would need to get prior consent from the individual to use or disclose personal data for a purpose that is in addition to, or different from, the purpose you originally obtained it for

11.3 Accurate and up to date – Personal data shall be adequate, relevant to the purpose or purposes for which they are processed. In practice, it means you should ensure that:
(a) You hold personal data about an individual that is sufficient for the purpose you are holding it for in relation to that individual
(b) You do not hold more information than you need for that purpose.

11.3.1 Therefore there is a requirement to identify the minimum amount of personal data that is needed to properly to fulfil the purpose it was collected for. This could include a requirement to collect more personal data than was originally anticipated. However, you should not hold personal data on the off chance that it might be useful in the future except for a foreseeable event that may never occurs e.g. Blood Group of a service user.

11.3.2 Personal data should not be collected or processed if it is insufficient for its intended process e.g. CCTV images that are poor quality, thereby making identification difficult.

11.3.3 Where sensitive personal data is concerned, it is particularly important to only collect or retain the minimum amount of information you need.

11.3.4 To comply with this principle you should:
(a) Take reasonable steps to ensure the accuracy of any personal data you obtain
(b) Ensure that the source of any personal data is clear
(c) Carefully consider any challenges to the accuracy of information
(d) Consider whether it is necessary to update the information.

11.3.5 Personal data is inaccurate if it is incorrect or misleading as to any matter of fact.
11.3.6 It is acceptable to keep records of events that happened in error, provided those records are not misleading about the facts. You may need to add a note to a record to clarify that a mistake happened.

11.3.7 Personal data should be kept up to date where the information is used for a purpose that relies on it remaining current e.g. A service users change of address.

11.3.8 It may be impractical to check the accuracy of personal data that someone else provides. You will not be considered to have breached this principle as long as:
(a) You have accurately recorded the information provided by the individual concerned, or by a third party
(b) You have taken reasonable steps in the circumstances to ensure accuracy of the information
(c) If the individual has challenged the accuracy of the information, this is clear to those accessing it.

11.3.9 If the information source is someone you know to be reliable, or is a well known organisation, it will usually be reasonable to assume they have given you accurate information, unless common sense suggests that there may be a mistake.

11.3.10 If a service user challenges the accuracy of information held about them you should consider whether the information is accurate and, if it is not, you should delete or correct it after satisfying yourself that the information was recorded incorrectly. (In the case of health records, the NMC guidelines on amending records must be followed)

11.3.11 An expression of an opinion about an individual is classed as their personal data. So when recording information about an individual, you should record whether it is an opinion, and, where appropriate, whose opinion it is. An area of particular sensitivity is medical opinion, where consultants routinely record their opinions about possible diagnoses, prior to tests being completed. An initial diagnosis may prove to be incorrect after an extensive examination or further tests. Individuals sometimes want the initial diagnosis to be deleted. However, the record accurately reflects the consultant’s diagnosis at a particular time, so is not inaccurate and does not need to be amended, especially if other subsequent activity was based on that opinion.

11.4 **Not kept longer than necessary** - Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes. In practice this means that you will need to:
(a) Review the length of time you keep personal data
(b) Consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it
(c) Securely delete information that is no longer needed for this purpose or these purposes
(d) Update, archive or securely delete information if it goes out of date.

11.4.1 Discarding personal data too soon would likely disadvantage the Priory and inconvenience the people the information is about.

11.4.2 Personal data will need to be retained longer in some cases than others. The appropriate retention period is likely to depend on the following:
(a) What the information is used for
(b) The relationship between the Priory and the individual
(c) Any legal or regulatory requirements
(d) Agreed industry practice

11.4.3 To determine the retention period of data refer to OP02.1 Document and Data Retention and divisional policies on record keeping.

11.5 **Processed in accordance with the rights of the data subject** - Personal data shall be processed in accordance with the rights of the data subject under this Act. Under the Act individuals have a right to:
(a) Access a copy of the information comprised in their personal data (see section 12 Subject Access Requests (SARs))
(b) Object to processing that is likely to cause or is causing damage or distress
(c) Prevent processing for direct marketing
(d) Object to decisions being taken by automated means
(e) In certain circumstances, to have inaccurate data rectified, blocked, erased or destroyed
(f) Claim compensation for damages caused by a breach to the Act.

11.5.1 An individual’s right to object to processing – An individual has a right to object to processing their data only if it causes unwarranted and substantial damage or distress. If it does they have a right to require an organisation to stop (or not to begin) the processing in question. An individual who wants to exercise this right has to put the objection in writing and state what they require you to do to avoid causing damage (financial loss or physical harm) or distress (emotional or mental pain). The extent to which you must comply is limited to:
(a) The individual can only object to you processing their own data.
(b) Processing the data must be causing unwarranted and substantial damage or distress and why the processing has this effect.

11.5.2 An individual has no right to object where:
(a) They have consented to the processing
(b) The processing is necessary:
   i) In relation to a contract that they have entered into
   ii) Because the individual has asked for something to be done so they can enter into a contract
(c) The processing is necessary because of a legal obligation that applies to you
(d) The processing is necessary to protect the individual’s vital interests.

11.5.3 The right to prevent direct marketing – Individuals have the right to prevent their data being processed for direct marketing. An individual can, at any time, give written notice to stop (or not begin) using their personal data for direct marketing. The Priory must stop processing for direct marketing within a reasonable period. It is a requirement that all electronic communications should stop within 28 days and postal communications within 2 months.

11.5.3.1 However, Priory Group will not use personal details of service users for marketing of any services that we provide. It will use geographic and personal records for internal marketing research, but not in any way outside the Priory Group.

11.5.4 Rights relating to inaccurate personal data – Where it is inaccurate an individual has a right to apply to the court for an order to rectify, block, erase or destroy the inaccurate information. Where the information in question has been provided by a third party, the Priory will not be considered to be in breach as long as:
(a) The information provided by the third party has been recorded correctly
(b) The Priory have taken reasonable steps to ensure the accuracy of the information
(c) If the individual has challenged the accuracy of the information, this is clear to anyone who accesses it.

11.5.5 This right also applies to personal data that contains an expression of opinion based on inaccurate personal data.

11.5.6 The right to compensation – If an individual suffers damage because Priory has breached the Act, they are entitled to claim damages. The Act allows Priory Group to defend a claim on the basis that all reasonable care in the circumstances was taken to avoid the breach. An individual who has suffered financial loss as a result of a breach is likely to be entitled to compensation.

11.5.6.1 An individual who has suffered distress alone will not usually be sufficient to entitle them to compensation. There are no guidelines about the level of compensation that an individual should receive. Where a request for compensation is received you should contact the Group Legal team for advice.
11.6.  **Protected by Appropriate Security** - 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 practice, Priory Group must have appropriate security to prevent the personal data that we hold being accidentally or deliberately compromised. (Also refer to OP27 Confidentiality and IT07 Printing, Photocopying, Scanning and Faxing, and divisional Record keeping policies with regard to security of records).

11.6.1 To meet this requirement Priory Group has deployed appropriate physical and technical security, which is backed up by robust policies and procedures.

11.6.2 Priory Group has the following systems in place to ensure that data is held securely:
(a) All hard-copy personnel files are held in secure lockable cabinets in the HR departments or Central HRD. The cabinets are locked when the offices are unoccupied.
(b) Any personal information transmitted electronically or transferred using electronic media must be encrypted using approved software or sent using NHS.net depending upon the sensitivity of the information transmitted in accordance with IT02 IT Security.
(c) Members of staff who have access to other staff member's personal information will be advised of the need to handle such information in accordance with this policy and of their contractual duty of confidence.
(d) The IT Network is protected by technical measures including firewalls and anti-virus software.
(e) Laptops and tablets are encrypted.
(f) All mobile devices are password protected with the ability to remote wipe if the device has been lost.
(g) All electronic data is held securely within systems and can only be created, amended or read by staff authorised to do so.
(h) All electronic data held in applications is backed up on a daily basis and replicated at our Disaster Recovery Centre.
(i) No hard copy records may be taken off site.
(j) The IT Network is protected from unauthorised external access using a Sonicwall Firewall and an SSL Sonicwall Aventail appliance which restricts connections to authorised systems on the internal network. Only users with a valid user account on the SSL Sonicwall Aventail appliance will be granted access. The password policy applied automatically by the network requires regular changing of users’ passwords and the use of complex passwords; refer to IT02 IT Security regarding further password requirements.

11.7 **Transfer Outside the European Economic Area** - Personal data shall not be transferred outside the EEA unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

11.7.1 Transfers overseas are unlikely to be lawful unless the country receiving the personal data has similar data protection laws to the UK, which currently only applies to members of the European Economic Area (EEA). Putting data on the worldwide web will involve transfers to countries outside the UK; software support by companies outside the UK may also involve data transfer outside the EEA.

11.7.2 Transferring personal data also includes information relating to individuals on paper.

11.7.3 Before making a transfer, you should consider whether you can achieve your aims without actually processing the data. For example, if the data is made anonymous so that it is not possible to identify individuals from it, now or in the future, then the DPA does not apply and a transfer can be made outside the EEA without any technical measures.

11.7.4 If there is a need to send personal identifiable information to countries outside of the EEA, this must be discussed with the Data Protection Advice team and the Chief Information Officer to ascertain the levels of protection for the information and if these can be assured.

11.7.5 Priory Group can transfer personal data overseas under the following conditions:
(a) Transfers of personal data overseas can be made with the express consent of the individual, which should be given clearly and freely and may later be withdrawn. Consent
will not be valid if the individual has no choice but to give their consent. The individual
must be told and have understood, the reasons for the transfer, the countries involved and
the risks involved.

(b) Personal data can be transferred overseas where it is necessary to carry out a contract
that the individual has entered into with Priory Group.

(c) Transfers of personal data may be completed where it is necessary for reasons of
substantial public interest. Substantial public interest is most likely to be relevant in the
prevention and detection of crime, national security and collecting tax. The public interest
must be that of the UK and not the country the personal data is transferred to.

(d) You can transfer personal data overseas where it is necessary to protect the vital interests
of the individual. This relates to matters of life and death.

(e) The personal data is required to be sent overseas in connection with any legal
proceedings, to obtain legal advice or to establish, exercise or defend legal rights. The
legal proceedings do not have to involve Priory Group or the individual as a party.

12 SUBJECT ACCESS REQUESTS (SARs)

12.1 Individuals have a right to inspect and have a copy of personal information that Priory Group
hold on them. In addition to a copy of the information, the data subject is also entitled to:

(a) A description of the purposes for which the data is being processed
(b) The recipients or classes of recipients to whom the data may be disclosed
(c) Any information available to the data controller as to the source of the data.

NB: If any of the information is obscure, perhaps due to a code or abbreviation, an explanation
must be provided.

12.2 Site or central services departmental managers are responsible for dealing with SARs in
accordance with divisional or departmental procedures and the requirements of the Data
Protection Act. However, for schools in Scotland, an SAR must be dealt with by the Operations
Director (as the representative of the proprietor of the school).

12.3 For a subject access request (SAR) to arise, the request must be in writing (letter, email or fax).
The information does not have to be provided until the appropriate fee has been paid and/or
the identity of the applicant has been verified. (See Subject Access Request Flowchart –
Appendix 1)

12.3.1 Where a person finds it impossible or unreasonably difficult to make a SAR in writing, you may
have to make reasonable adjustment for them under the Disability Discrimination Act. This
could include treating a verbal request for information as though it was a valid request. You
might also have to respond in particular format which is accessible to the person, such as
Braille, large print etc. (For translations or different formats contact the Marketing team).

12.4 All such requests must be responded to within 40 calendar days of receiving the request and
payment. The maximum fee that can be charged is £10 (up to £50 for health or education
records). The deadlines for responses to SARs must be adhered to. If there is any doubt about
what to do or by when, then sites should contact the Data Protection Advice team for
assistance.

12.4.1 No charge will be made if the data subject prefers to view their records on site, with no hard
copy being provided.

12.5 Staff must verify the identity of the applicant before sending them information. Requests may
be received from a third party on behalf of an individual e.g. solicitor, relative. In these cases
you need to be satisfied that the third party has written authority to act. (Refer to 17.8)

12.6 Where Priory Group reasonably requires further information in order to be satisfied about the
identity of the person making the request, the applicant must be informed of this in writing as
soon as possible. The request does not have to be complied with until the further information
is supplied. The Data Protection Advice team can be contacted with queries or for further
advice.
12.7 With regard to information, other than that contained within a service user record, the right of access is only to information held by Priory Group in an electronic form or, in a file that is sufficiently indexed to enable any personal information to be located within it relatively easily (properly known as a "relevant filing system"). Members of staff should realise that it is unlikely that any manual personnel file would amount to such a relevant filing system and therefore they do not have an automatic right of access to the personal data contained within it.

12.8 For the avoidance of doubt a service user does have a right of access to his/her records, subject to exceptions dealt with below.

12.8.1 Where Priory Group cannot comply with the request without disclosing information that would identify another person (the "third party"), then that information should be deleted or redacted from the information provided to the requestor unless:
   (a) The third party has consented to the disclosure of the information to the applicant.
   (b) It is reasonable in all the circumstances to comply with the request without the consent of the third party. What is reasonable in all the circumstances requires particular consideration to be given to the following factors:
      i) Any duty of confidentiality owed to the third party.
      ii) Any steps taken by Priory Group with a view to seeking the consent of the third party.
      iii) Whether the third party is capable of giving consent; and
      iv) Any express refusal of consent by the other individual.
   (c) The circumstances in paragraph 17.5 apply.

12.8.2 Where information about a third party will be disclosed then the approval of the Data Protection Advice team must be obtained in advance.

12.10 The information to which an applicant has a right of access must be supplied in permanent form, which could mean a copy of the relevant document or creating a new document containing the information or an electronic document unless it would involve disproportionate effort or the applicant agrees otherwise. Usually, information will be provided in the form of a copy document with deletion of any information to which the application is not entitled.

12.11 Requests for information about children - Even if a child is too young to understand the implications of subject access rights, data about them is still their personal data and does not belong to a parent or guardian. So it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility. Before responding to a SAR for information held about a child, you should consider whether the child is mature enough to understand their rights. If you are confident that the child understands their rights, then you should respond to the child rather than a parent.

12.11.1 When considering cases you should take into account, among other things:
   (a) The child's level of maturity and their ability to make decisions
   (b) The nature of the personal data
   (c) Any court orders relating to parental access or responsibility that may apply
   (d) Any duty of confidence owed to the child or young person
   (e) Any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment
   (f) Any detriment to the child or young person if individuals with parental responsibility cannot access the information
   (g) Any views the child or young person has on whether their parents should have access to information about them.

12.11.2 In Scotland, the law presumes that a child aged 12 years or more has the capacity to make a subject access request. The presumption does not apply in England, Wales and Northern Ireland, but it does indicate an approach that would be considered reasonable in most cases.

12.12 Data that includes information about other people – responding to a SAR may involve providing information that relates both to the individual making the request and to another
individual. The Act says that you do not have to comply with a request if to do so would mean disclosing information about another individual who can be identified from that information, except where:

(a) The other individual has consented to the disclosure; or
(b) It is reasonable in all circumstances to comply with the request without the individual’s consent.

12.13 Repeated or unreasonable requests – The Act does not limit the number of SARs that an individual can make to an organisation. You do not have to comply with an identical or similar request to one you have already dealt with, unless a reasonable interval has elapsed. To consider whether a request has been made at a reasonable interval you should consider the following:

(a) Whether the data is particularly sensitive
(b) If the processing is likely to cause detriment to the individual
(c) Whether the data is unlikely to have changed between requests.

13 INDIVIDUAL’S CONSENT

13.1 There are circumstances under which it is sufficient to inform an individual and thereby gain their ‘implied consent’. In some other circumstances their ‘explicit consent’ should be obtained.

13.2 Priory Group and members of staff must always ensure that an individual is aware of what is going to happen to the personal information that they provide. For example, a service user should be made aware when information is going to be passed to their general practitioner or to a professional outside Priory Group to enable the provision of further care/treatment/support/education. Where any disclosure is going to take place to an individual or organisation outside Priory Group, in a context not connected with the care of a service user or routine staff administration matters (such as payroll or disclosure to the Inland Revenue), then the individual’s written consent must be obtained in advance of any such disclosure.

13.3 However, an individual’s consent is not always required to process personal information about him or her, provided that:

(a) The individual is already aware, in general terms, of the particular purpose for which the information is to be used; and
(b) The processing is necessary or required by law; and
(c) The processing is consistent with any other applicable law, for example, the law of confidentiality.
(d) Disclosure is justified in the public interest.
(e) The data is anonymised.

13.3.1 For example, for personal information other than sensitive personal data, processing may take place where it is necessary for the performance of a contract to which the service user or staff member is a party (for example, an employment contract). This makes practical sense as it demonstrates that there is no need to obtain a member of staff’s permission every time information is sent to payroll, for example. The processing is also permissible where it is necessary for the business purposes of Priory Group although such processing would not take place where it was unwarranted in any particular case if it would prejudice the rights or some other legitimate interest of the individual concerned.

13.4 In relation to sensitive personal data, explicit consent to processing must be obtained from the service user. Explicit meaning that the individual has been fully informed about the uses of the data and any potential disclosures and their agreement has been secured. As a matter of policy this agreement must be recorded in writing. However, consent is not always required but in addition to the circumstances set out in paragraph 16.4 above, the following criteria needs to be met:

(a) The processing must be necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on Priory Group in connection with employment
(b) The processing is necessary for medical purposes and is undertaken by a health professional or another member of Priory Group staff who will owe a similar duty of confidentiality to the individual. Medical purposes include the purposes of preventative
medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

13.5 This allows the day-to-day functioning of Priory Group to take place without requiring an individual’s specific agreement each time their personal information is passed between those responsible for their care/treatment/support or education.

13.6 There are other circumstances where processing without consent is permissible. However, in all other cases or where there is any concern about whether personal information is being processed lawfully, the advice of the Data Protection Advice team must be sought, unless it is immediately necessary to process personal information to protect anyone’s mental or physical health or where anyone’s life could be at risk.

14 DISCLOSURE OF PERSONAL INFORMATION

14.1 Personal information will not be disclosed outside Priory Group unless to do so is consistent with this policy and the fair processing of information (see paragraph 11.1) unless, there is a statutory obligation to do so, it is otherwise lawful or the individual has given his/her consent to the disclosure.

14.2 In giving consent the individual must be informed of the extent of any disclosure and its implications. In all cases no more information will be disclosed than is necessary to achieve the purpose behind the disclosure.

14.3 The duty to obtain consent is not absolute, but can only be overridden if the “Data Controller” can justify disclosure on the grounds that the public interest in maintaining confidentiality is outweighed by the public interest in making the disclosure (for example in order to protect the vital interests of the data subjects or another person, or for the prevention and detection of crime). Before making any such disclosure, the proposed disclosure should be discussed with Data Protection Advice team and in the case of doubt about the legality of disclosure, legal advice should be sought.

14.4 There are statutory obligations to disclose, i.e. information must always be disclosed if required by legislation/statute or court order e.g. notifications of communicable diseases, abortion, substance misuse, etc.

14.5 There are statutory restrictions on the disclosure of information relating to HIV and AIDS, other sexually transmitted diseases, assisted conception and assisted abortion.

14.6 Public Interest Disclosure Act 1998 is designed to protect employees who make certain disclosures of information in the public interest by amending the Employment Rights Act 1996. It offers protection against reprisals/victimisation of staff who disclose information (usually to their employer) which, in the reasonable belief of the worker making the disclosure, tends to show the occurrence or likely occurrence of:
(a) A criminal offence
(b) A person’s failure to comply with any legal obligation
(c) A miscarriage of justice
(d) The health and safety of an individual being endangered
(e) Damage to the environment.

14.7 It also includes information tending to show any matter relating to 14.3 that has been, is being or is likely to be deliberately concealed. Such disclosures are defined as qualified disclosures for the purposes of the Public Interest Disclosure Act. The DPA makes provision for it to be overridden if there are public interest reasons why data protection should not apply, but any disclosure must be justifiable and recorded.

14.8 There may be circumstances in which personal data may need to be used in responding to a major incident or dealing with a risk to public health. A decision to use information relating to individual people would only be taken by the incident control team if judged to be in the public interest to do so.
14.6 Requests from the police (or the NHS Counter Fraud Service) would normally be refused. However, exemption under Section 29 of the DPA allows disclosure in the public interest, at the discretion of the “Data Controller”, for the prevention or detection of crime. The request must be in writing, justifying the grounds for disclosure, and submitted to the appropriate School Principal/Hospital Director/Registered Home Manager/Service Manager or Specialist Director.

14.7 Where service user information is to be used in research the “data subject” (i.e. the service user to whom the information relates) should be informed about the intended use of this information before disclosure takes place. This applies irrespective of whether or not the results are to be made available to the service user in a form that identifies them (with their consent).

14.8 Disclosures of information about deceased persons will be handled as ‘Subject Access requests’ under the surviving part of the Access to Records Act (see Appendix 1 – Subject Access Request Flowchart).

15 ANONYMISING INFORMATION

15.1 The removal of personal details alone may be sufficient to protect an individual’s identity when disclosing information. If anonymisation is to be relied upon as the condition for disclosure without consent, it requires the removal of any information that could allow identification of a living individual.

15.2 For some uses of data, the retention of a hospital number or other tracking code, may be acceptable if recipients of the data do not have access to the ‘key’ to trace the identity of the service user. Such anonymisation may, with appropriate safeguards, be sufficient to allow use without express consent. It is good practice to inform people that their information may be used anonymously for audit purposes.

16 SHARING INFORMATION BETWEEN ORGANISATIONS

16.1 Service user information should only be shared between organisations that have adopted an appropriate policy.

16.2 The principles governing the sharing of personal information are essentially the same as those governing its use within an organisation. The difference is in the extent to which control measures need to be taken and made explicit. The responsibilities for protecting the confidentiality of service user information extend to any individuals and agencies to whom information is passed. Furthermore, such information may only be used for the specific purpose for which it is shared. The organisation releasing (or disclosing) the information is responsible for ensuring that the recipient keeps it secure and confidential, and uses it only for the agreed purpose.

16.3 Business Information - All information concerning the operations of Priory Group and all companies within it, is confidential. Information relating to the business may only be disclosed when specifically authorised by Directors. Priory Group has copyright and design rights on publications, assessment formats, forms and data systems. These may not be published or shared with any other organisations without the express written permission of the Directors.

17 DATA PROCESSORS

17.1 Where personal information is to be processed on behalf of Priory Group the following requirements must be met:
   (a) There must be a written contract.
   (b) The contract must provide that the data processor will only act on instructions from Priory Group.
   (c) The contract must provide that the data processor will comply with the requirements for appropriate, technical and organisational measures which must be taken against
unauthorised or unlawful processing of personal data and against accidental loss of
destruction of, or damage to, personal data.

17.2 Unless a data processor can demonstrate the appropriate security measures referred to above
and unless a contractual guarantee is provided that the compliance with those measures will be
in place then Priory Group will not enter into the contract with that data processor.

17.3 **Provision of Health Information** - There are additional provisions with regard to personal
information about someone’s physical or mental health or condition. It is important to note that
a service user has a right of access to the information contained in his/her health records,
subject to certain exemptions. These special provisions apply not just to health records but to
information wherever it is recorded about someone’s health or condition.

17.4 There is no right of access to health information to the extent to which it would be likely to
cause serious harm to the physical or mental health or condition of the service user or any
other persons (including the health care professionals concerned with the person’s treatment).
It is the responsibility of the health professional who is currently or was most recently
responsible for the clinical care of their service user in relation to those particular records, to
make the decision on this issue. Where no such health professional is available, then it must be
a health professional who has the necessary experience and qualifications to advise on this
issue and in these circumstances it will be determined by the Chief Medical Officer.

17.5 Priory Group will not release health information to an applicant falling in the following groups:
(a) Information provided by the person in the expectation that it would not be disclosed to the
applicant.
(b) Information obtained as a result of any examination or investigation to which the person
consented in the expectation that the information would not be disclosed to the applicant.
(c) Information which the person has expressly indicated should not be disclosed to the
applicant.

17.6 This proviso does not apply to the extent that the request relates to information, which Priory
Group is satisfied has previously been seen by the applicant or is already within the knowledge
of the applicant, perhaps because he or she provided the information. Furthermore, if in the
previous six months the appropriate health professional has already given an opinion that the
exemption applies then there is no need to re-consult unless it is reasonable in the
circumstances to do so.

17.7 The restrictions on the identification of third parties when disclosing health information does not
apply to identification of a health professional who has compiled or contributed to a service
user’s health record or has been involved in the care of the service user in his or her capacity as
a health professional.

17.8 **Request for Data by a Third Party** - No one other than the service user has a right to his or
her personal information (apart from the points raised above about children and adults without
capacity). However, others may be appointed to act as agents for the service user, such as
solicitors or relatives. In such circumstances, written authorisation from the data subject must
be obtained prior to the release of any personal information to the agent. **OP Form: 08A**
Access to Personal/Sensitive Information - Authority from Data Subject is available for this
purpose, or follow divisional procedures and use divisional documentation.

17.8.1 Priory Group must be satisfied that the service user is aware of what he or she is consenting to
in these circumstances. In cases of doubt, the Data Protection Advice team must be consulted.
In all other cases, consideration needs to be given to whether it is lawful to process the data
and therefore, whether or not it is necessary to provide information to the individual making the
request. For example, in rare cases, a request for information may be received from the police
if they are investigating a serious crime. There are circumstances where it would be lawful to
provide the information, but no such disclosure must take place without consulting with the
Data Protection Advice team.
17.9 Enquiries from relatives and friends should be handled in accordance with the wishes (consent) of the service user, taking care to positively identify the enquirer. No-one with access to confidential information shall pass on any information to their relatives or friends, or seek to find out details about themselves. No information shall be passed on for personal or commercial gain. Disciplinary action can be taken against staff and healthcare professionals if this is breached.

18 EXEMPTIONS

18.1 There are some exemptions from the Act to accommodate special circumstances in respect of disclosure and non-disclosure.

18.1.1 It is sometimes appropriate to disclose personal data for certain purposes to do with criminal justice or the taxation system. In particular where personal data is processed could assist in:
(a) The prevention or detection of crime
(b) The capture or prosecution of offenders
(c) The assessment or collection of tax or duty.

18.1.2 Personal data processed for any of these purposes is exempt from:
(a) An organisation’s duty to comply with data protection principle 1, but not including the duty to satisfy one or more of the conditions for processing; and
(b) An individual’s right to make a subject access request. This is to ensure that any investigation or investigation is not prejudiced by disclosing the information to the data subject.

18.1.3 The Act provides an exemption for processing data in connection with regulatory activities. This exemption is not available to all organisations and it applies only to bodies that perform public regulatory functions concerned with:
(a) Protecting members of the public from dishonesty, malpractice, incompetence or seriously improper conduct or in connection with health and safety
(b) Protecting charities
(c) Fair competition in business.

18.1.3.1 For the exemption to apply, those functions must also be
(a) Conferred by or under an enactment
(b) Functions of the Crown, a Minister or government department
(c) Any other public function exercised in the public interest.

18.1.4 Where an organisation is obliged by or under an enactment to make information available (by publishing) to the public, personal data that is included in that information is exempt from:
(a) The subject information provisions;
(b) The non-disclosure provisions;
(c) The organisations duty to comply with data protection principle 4, accuracy
(d) An individual’s right in certain circumstances to have inaccurate personal information rectified, blocked or erased or destroyed.

18.2 Disclosures Required By Law - Personal data is exempt from non-disclosure if you are required to disclose it:
(a) By or under a UK enactment
(b) By any rule of common law
(c) By an order of a court or tribunal in any jurisdiction.

18.2.1 In these circumstances the legal obligation overrides any objection the individuals may have.

18.3 Legal Advice or Proceedings - Personal data is exempt from non-disclosure where the disclosure of the data is necessary:
(a) For or in connection with any legal proceedings (including prospective legal proceedings)
(b) For obtaining legal advice
(c) For establishing, exercising or defending legal rights.
18.3.1 You do not have to disclose personal data in response to a third party. You can choose whether or not to apply the exemption and should only do so where you are satisfied that the disclosure falls within the scope of the exemption. Alternatively you may choose not to comply with the request and only do so if obliged by a court order.

18.4 **Confidential References** - Personal data is exempt from an individual's right of subject access if it comprises a confidential reference that an organisation gives in connection with education, training or employment, appointing office holders, or providing services. The exemption does not apply for references that an organisation receives.

18.5 **Management Information** - Personal data that is processed for management forecasting or management planning in respect of an individual is exempt as it would be likely to prejudice the business or other activity of the organisation. Example: If a business was planning a reorganisation then the business would be exempt from having to disclose the plans to an individual.

18.6 **Negotiations** - Personal data that consists of a record of an organisation's intentions in negotiations with an individual do not have to be disclosed as it could prejudice the outcome. Example: A personal injury claim settlement, where the insurance company are disputing the serious of the claim and the offer they are prepared to make.

18.7 **Domestic Purposes** - Data is exempt where it is stored and processed by an individual only for the purposes of their personal, family or household affairs.

18.8 **Other Exemptions** - Exemptions are also available in relation to:
(a) National security and the armed forces
(b) Personal data that is processed only for journalistic, literary or artistic purposes;
(c) Personal data that is processed only for research, statistical or historical purposes;
(d) Personal data relating to an individual's physical or mental health. This applies only in certain circumstances and only if granting a subject access would be likely to cause serious harm to the physical or mental health of the individual or someone else;
(e) Personal data that consists of educational records or relates to social work;
(f) Personal data relating to human fertilisation and embryology, adoption records and reports, statements of a child's special educational needs and parental order records and reports;
(g) Personal data processed for, or in connection with, a corporate finance service involving price-sensitive information;
(h) Examination marks and personal data contained in examination scripts; and
(i) Personal data processed for the purposes of making judicial, Crown, or Ministerial appointments or for conferring honours.

19 **AUDIT**

19.1 An audit of Data Protection processes will be conducted by all departments/sites twice a year as a minimum using **OP Form: 08B**

20 **REFERENCES**

20.1 Data Protection Act 1998 - See Website: [http://www.ico.gov.uk](http://www.ico.gov.uk)
Access to Health Records Act 1990
Employment Rights Act 1996
Public Interest Disclosure Act 1998
Caldicott, F (2013) Information: To share or not to share? The Information Governance Review
DH (2013) Information: To share or not to share? Government response to the Caldicott Review
ICO (2014) Subject Access Code of Practice: Dealing with requests from individuals for personal information
APPENDIX 1 – Subject Access Request Flowchart
APPENDIX 2 – Information Sheet for New Staff (OP Form: 11)

Associated forms:
OP Form: 08 Using and Sharing Information About You
OP Form: 08A Access to Personal/Sensitive Information - Authority from Data Subject
OP Form: 08B Data Protection Audit
OP Form: 08C Using and Sharing Information About You – Easy Read
OP Form: 10 E-mail Acceptance Declaration
OP Form: 11 Data Protection and Service User Information

Also see divisional forms and letters associated with Record Keeping and Access to Records
APPENDIX 1

SUBJECT ACCESS REQUEST FLOWCHART

Request for Personal Information Received
Determine whether this request should be treated as a routine enquiry or as a Subject Access Request

YES
Any written enquiry that asks to information that we hold about the person making the request can be construed as a subject access request.  
* e.g. “Please send me a copy of my staff records”  
* “I have the right to see all the invoices issued to me for the last three years. Please send me copies”  
* “I am a solicitor acting on behalf of my service user and I request a copy of the medical records. An appropriate letter of authority is enclosed”

Check the requesters’ identity.  
Often you will not need to do this because they may be someone you have regular contact with, and know the address. However, if you doubt their identity you can ask them to provide evidence to confirm it – e.g. a piece of evidence held in their records that only they would know such as next of kin details.  
If the requester is a third party, check that you have the authority of the person that the information is about, before you provide any information.

NO
In many cases there will be no need to treat the request as a Subject Access Request. If you would usually deal with the request in the normal course of business, then do so.  
* e.g. “Can you tell me what my hospital number is please? I have a query on my last invoice, can you let me know what the amount was for?”

Handle the query as part of your usual course of business following any Confidentiality or Data Protection policies as normal.

Other necessary Information
You will need to ask the requester for any other information you need to find the records they want promptly as these may be in several different places.  
You may have quite a wide search if they can’t narrow down their request.  
You have 40 days to respond to a Subject Access Request after receiving all the information you need and any fee.

Fees
The maximum Priory can charge for a Subject Access Request is £10 unless the request covers Medical or Educational Records. If these records are held on computer, the maximum charge is £10, but if the records are a mixture of computer and manual, then the Priory can charge up to £50. If you need a fee you must ask the requester promptly for one.

40 Days Response time
The 40 calendar days in which you must respond starts when you have received the fee and all necessary information to help you find the records.

Check all Computer and Manual Records to see if Priory holds any information about the individual

YES
Routine changes to the information can be made in the normal course of business, but changes MUST not be made as a result of receiving the request, even if inaccurate or embarrassing information is found within the record.

NO
If you hold no personal information about the individual you must tell them this in writing

References to Third Parties
The Priory does not have to supply this information unless the other people mentioned have given their consent or it is reasonable to supply information without their consent. Even when other people’s information should not be disclosed, Priory should still supply as much information as possible by obtaining consent or removing other people’s names and other identifying information.
Exempt Information

There may be circumstances in which Priory is not obliged to supply certain information. Some of the most important exemptions apply to:

- Crime prevention and detection
- Negotiations with the requester
- Management forecasts
- Confidential references given by you (but not to you)
- Information used for research, historical or statistical purposes
- Information covered by legal professional privilege e.g. the consultant can withhold medical information if disclosure to the requester would cause a significant danger to the requester or to a third party

Complex terms or codes

The information may include abbreviations, medical or technical terms that the individual will not understand, for CRB, HoNOS. You must make sure that these are explained so that the information can be understood. The best way is to provide a glossary.

Preparing the Information to be sent

A copy of the information should be supplied in a permanent form except where the requester agrees or where it is impossible to do so, or would involve undue effort. This could include very significant cost or time taken to provide the information in hard copy form. An alternative would be to allow the requester to view the information on screen.

Remember: Priory Group have 40 days to comply with the request starting from when you receive all the information necessary to deal with the request and any fee.

Individual can complain to the Information Commissioners' Office or apply to a court if Priory does not respond within this time limit.

Hand the information to the requester in person, or post to an agreed address.

If ALL the information that you hold is exempt you can reply by telling them that you do not hold any information that you are required to reveal.

If some of the information is exempt then this does not need to be included in the response.
APPENDIX 2 – Information sheet for new staff (OP Form: 11)

DATA PROTECTION AND SERVICE USER INFORMATION

This document must be read in conjunction with the Priory Group policy
OP02 Data Protection:

Personal information will be obtained from service users while using the services provided by Priory Group. Some of the information will be of an administrative nature such as their name, address and contact details. Other information may be about their mental and physical health. Generally speaking, information obtained from a service user will be held in confidence by Priory Group. Individual members of staff may also owe legal and ethical obligations of confidentiality to service users when information is provided to them. Personal information, whether it is confidential or not, must also be dealt with in accordance with the Data Protection Act. Consultants and therapists may also maintain their own independent records of contact with service users. In such cases it is the clinician’s responsibility to inform the service user and comply with his/her own legal obligations.

As a general rule, confidential information must not be processed without the service user’s explicit consent unless the processing can be justified in the substantial public interest or there is some other legal basis for using the information, such as a Court order or statutory obligation. Under the Data Protection Act, provided the service user has been informed in general terms of the purposes for which their information is going to be used (as well as the other criteria set out in OP02 Data Protection) then personal information may be processed.

However, personal information from which the service user might be identified should not be used for the purposes of any kind of research without the service user’s explicit consent.

In respect of service users, there are many circumstances where confidential information about them is shared between professionals in the course of providing care (health) for the service user. It is not necessary to obtain a service user’s explicit consent on each occasion provided that the service user is generally aware that information is going to be passed in this way. For example, it is not necessary to obtain a service user’s explicit consent every time a healthcare professional writes to a general practitioner. However, service users must be aware that such exchanges are likely to take place and if a service user withdrew their consent for such correspondence, then that should be respected. Another example would be information provided to a service user’s funding organisations in order for Priory Group to obtain reimbursement. However, when a referral to a hospital is not from the service user’s GP the service user must be asked to sign a form to give or refuse consent for sending details of the treatment provide to his/her GP.

In order that service users are sufficiently informed about the purposes to which their information will be put the information leaflet OP Form: 08 will be supplied to each new service user upon contracting services from the Priory Group.

In compiling and processing service user records the principles set out in the policy OP02 Data Protection must be followed. In terms of handling service users’ personal information within Priory Group the following additional points should be followed (based on the Caldicott principles for health and social care records):
(a) Truly anonymised information should be used wherever it can be. For example, for the purposes of audit or administration.
(b) If it is not possible to use truly anonymised information and there is a requirement to be able to “track back” then rather than using information that can directly identify a service user, a unique identifier should be used, for example, a service user number.
(c) In general terms and wherever possible and practicable, a service user’s explicit consent should be obtained for the passage of information. The less directly connected with the service user’s care the passage of information is, the more the requirement. In any case,
where information is passed without explicit consent, you must be able to justify why that consent has not been obtained.

(d) Justify the purpose(s) of using the service user’s data.

(e) Use the minimum person-identifiable information necessary for the purpose.

(f) Access to person-identifiable information must be on a need to know basis.

(g) Members of staff must be aware of their responsibilities and obligations with regard to confidentiality.

(h) Members of staff must understand and comply with the law as set out in this policy.

If a service user refuses their explicit consent to a particular use or disclosure of information, then it is the responsibility of the staff member in charge of their care/support/education to ensure that they have been provided with full information as to the consequences of their refusal. Such circumstances must be recorded in writing together with the explanation that has been given and the service user should be asked to initial the note to acknowledge that they have received the information and understood it and the consequences of their refusal.

If a circumstance arises where any service user information is to be transferred outside Priory Group in circumstances that are not covered by part of OP02 Data Protection, then before any such transfer of information takes place the Data Protection Advice team must be consulted.

Service users have a right of access to their personal information and/or health/social care/education records.

A service user’s personal information and records will be retained in accordance with the policy OP02 Data Protection. All records for destruction will be disposed of securely.

(After reading, a signed copy of this letter should be sent to the HR department).

Signed…………………………………… Name……………………………………. Date……………………..