Prospect Surgery

Information Governance Policy

Contents

1. Introduction … … … … … … … … … … … 3

2. Definitions… … … … … … … … … … … … 3

3. Responsibilities … … … … … … … … … … … 3

4. Principles … … … … … … … … … … … … 3

5. Data Protection Act … … … … … … … … … … 5

6. Freedom of Information Act … … … … … … … … 6

7. Information Commissioner's Office … … … … … … … 6

8. Security … … … … … … … … … … … … 6

9. Access to Health Records … … … … … … … … … 6

10. Record Keeping and Retention … … … … … … … … 6

11. Key Reference Documents … … … … … … … … 6

Appendix 1 … Data Protection Policy … … … … … … 7
Appendix 2 … Access to Medical Records Policy … … … … 12
Appendix 3 … Information Security Policy … … … … … 23
Appendix 4 … Record Keeping, Storage, Retention and Destruction of Medical Records Policy … … … 29

1. Introduction

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.

It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management.

2. Definitions

Caldicott Guardian – A Caldicott Guardian is a senior person responsible for protecting the confidentiality of a patient and service-user information and enabling appropriate information-sharing. The Caldicott Guardian plays a key role in ensuring that the NHS, Councils with Social Services responsibilities and partner organisations satisfy the highest practicable standards for handling patient identifiable information.

3. Responsibilities

Caldicott Guardian - Dr S Sabir, Senior Partner

Clinical Governance Lead – Mrs Jayne Henderson , Practice Manager

All staff - have a responsibility to ensure that they are working to the most up to date and relevant policies and procedures. By doing so, the quality of services offered will be maintained and the chances of information security and confidentiality being breeched will be minimised.

4. Principles

The Practice recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Practice fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information. The Practice also recognises the need to share patient information with other health organisations and other agencies in a controlled manner, consistent with the interests of the patient and, in some circumstances, the public interest.

The Practice believes that accurate, timely and relevant information is essential to deliver the highest quality healthcare. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision making processes.

There are four key interlinked strands to the Information Governance Policy:-

- Openness
- Legal compliance
- Information security
- Quality assurance

Openness

Non-confidential information on the Practice and its services should be available to the public through a variety of media, in line with the Practice's code of openness.

The Practice will establish and maintain policies to ensure compliance with the Freedom of Information Act 2005

The Practice will undertake or commission annual assessments and audits of its policies and arrangements for openness.

Patients should have ready access to information relating to their own health care, their options for treatment and their rights as a patient.

The Practice will have clear procedures and arrangements for liaison with the press and broadcasting media.

The Practice will have clear procedures and arrangements for handling queries from patients and the public.

Legal Compliance

The Practice regards all identifiable personal information relating to patients as confidential.

The Practice will undertake or commission annual assessments and audits of its compliance with legal requirements.

The Practice regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

The Practice will establish and maintain policies to ensure compliance with the Data Protection Act 2018, Human Rights Act (Amendment) Order 2004 and the common law confidentiality.

The Practice will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of

relevant legislation [Health and Social Care Act 2015, the Antisocial Behaviour Crime and Policing Act 2014 and The Children's Act 2004).

Information Security

The Practice will establish and maintain policies for the effective and secure management of its information assets and resources.

The Practice will undertake or commission annual assessments and audits of its information and IT security arrangements.

The Practice will promote effective confidentiality and security practice to its staff through policies, procedures and training.

The Practice will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

Information Quality Assurance

The Practice will establish and maintain policies and procedures for information quality assurance and the effective management of records.

The Practice will undertake or commission annual assessments and audits of its information quality and records management arrangements.

Managers are expected to take ownership of, and seek to improve, the quality of information within their services.

Wherever possible, information quality should be assured at the point of collection.

Data standards will be set through clear and consistent definition of data items, in accordance with national standards.

The Practice will promote information quality and effective records management through policies, procedures, user manuals and training.

5. Data Protection Act [DPA] 2018

As Practices handle information about individuals, they have a number of legal obligations to protect that information under the DPA.

Appendix One provides further information about the DPA, or visit the website: https://ico.org.uk/for-organisations/guide-to-data-protection/

6. Freedom of Information Act [FOIA] 2014

General Practice has a legal obligation to provide some types of information under the FOIA. See Appendix One – Data Protection Policy, or visit the website: https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

7. Information Commissioner's Office

The Information Commissioner's Office is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

All GP Practices are required to register as a "Data Controller" with the ICO and renew their registration annually. For more information about registration visit the website:
https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/y

8. Security

See Appendix Two – Information Security Policy.

9. Access to Health Records

See Appendix Three – Access to Health Records.

10. Record Keeping and Retention

See Appendix Four – Policy and protocol for record keeping and the storage, retention and destruction of health records.

Appendix One

Data Protection Policy

1. Introduction

The Data Protection Act 2018 [the DPA] was introduced to regulate the use of automatically processed information relating to individuals and the provision of services in respect of such information. It therefore relates to any information about any identifiable person that is held on any form of computer equipment storage device.

There are many points to consider regarding any organisation's compliance with the DPA, data access, registrations and commitment to the eight Principles of the DPA for example. The eight Principles of the DPA are incorporated within this policy and are shown in point 3, below.

This policy sets out the Practice's approach to compliance and the responsibilities and processes thereof. This policy should be read in conjunction with the Practice Policies on confidentiality and the data base security.

2. Roles and Responsibilities

The Practice Manager is responsible for implementing the DPA and ensuring compliance.

Individuals are responsible for liaising with the Practice Manager on all aspects of data protection as it relates to their duties.

Every member of staff has responsibilities demanded by the DPA. Under certain circumstances any member of staff may be held personally liable for acts carried out in the normal course of their duties. All staff must treat personal information with care and ensure they do not pass it on to unauthorised persons. If an individual is found to have made any unauthorised disclosure of personal information they can face prosecution and disciplinary action.

Staff wishing to use non-Practice computers, including home computers for any aspect of NHS business must ensure by discussion with the Practice Manager or Deputy Manager that their proposed activities do not compromise the Practice's compliance with the DPA.

3. Principles of the Data Protection Act 2018

The Principles state that:

Principle 1 - The information contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully.

Principle 2 - *Personal* data shall be held only for one or more specified and lawful purpose.

Principle 3 - Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or purposes.

Principle 4 - Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes.

Principle 5 - Personal data shall be accurate and, where necessary, kept up to date.

Principle 6 - Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.

Principle 7 - An individual shall be entitled at reasonable intervals and without undue delay or expense:

- to be informed by a Data User whether he/she holds personal data of which that individual is the subject.
- to have access to any such data held by a Data User: and
- where appropriate, to have such data corrected or erased.

Principle 8 - Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data.

4. Registration

The Practice as a whole is a registered Data User. It is the responsibility of the Practice Manager to register and to maintain all registrations for all of the Practice's electronically held personal data. These registrations define what personal data the Practice holds electronically, the reason(s) it is held and who can have access to it.

If an individual is uncertain about who can have access to the personal data they work with it is their responsibility to ask the Practice Manager.

5. Data Access Requests

The basic rules for handling access are specified in Section 21 of the Act, subject to the modifications introduced by the Orders made under the Act. The core of this section is:

"An individual shall be entitled:-

[i] To be informed by the Data User whether the data held by the Data User includes any personal data of which that individual is the Data Subject, and

[ii] To be supplied by a Data User with a copy of the information constituting any such personal data held by the Data User'

[iii] and where any of the information referred to in Paragraph [ii] is expressed in terms which are not intelligible without explanation, the information shall be accompanied by an explanation of those terms" (Act Section 21 (1))

The legal requirement is such that the Practice must respond only when one of the following applies:

- The request is made by the data subject him/herself.
- The request is made on behalf of the data subject who has given written authorisation for the applicant to proceed.
- The request is made on behalf of a child where the Data User, on the advice of an appropriate Health Professional, is satisfied that the child is unable to understand the nature of the request. The request must be in the interest of the child not just the parents.

It is the intention of the Practice to be as helpful as possible to individuals seeking access to their personal data. However, in the event that the Practice has not received signed authorisation, the Practice can decide whether or not to release the information and is not bound by the normal legal deadlines or fees.

The DPA imposes a forty day; elapsed time deadline for compliance from the time a Data User receives a valid, written request containing sufficient details for the required personal data to be located. Any requests for access to the Practice electronically held data must be processed immediately. It is the responsibility of any member of staff opening a written access request to date stamp its receipt and pass on to the Secretary or a designated deputy immediately. In the event that the request is verbal advice should be sought from the Deputy Practice Manager.

The Secretary is responsible for ensuring requests are logged and the necessary paperwork completed.

When the Secretary is satisfied that the access request is valid the request should be notified to the relevant Health Professional.
The Health Professional will review the record to ensure that the most appropriate information is included and to avoid improper disclosures. If there are difficulties the Practice Manager will seek advice of the Data Protection Registrar.

Where there is the potential for serious mental or physical harm caused by the release of the information, the Health Professional will remove the specified information from the Practice response to the access request. The Health Professional will record his/her clinical judgement in the clinical record.

The Secretary is responsible for ensuring the personal data is edited so that no un-consenting third party is identified. The Practice is committed to giving as much information as possible without revealing the identity of any other individuals who are not Health Professionals. The Secretary will therefore ensure that the minimum amount of information necessary to conceal the other individual's identity is edited out of the personal data.

Access request logs and a copy of any personal data issued to the requester must be held for six years in a secure, locked filing cabinet, located in the Surgery.

6. Data Access Requests under the Freedom of Information Act [FOIA] 2014

The FOIA came into force on 1 January 2005. It provides a public right of access to all types of recorded information held by public authorities. General Practices have a statutory duty to comply with the FOIA.

Prospect Surgery recognises the importance of the FOIA, and will ensure that appropriate systems are put into place to publicise what recorded information is held by the Practice and how this information can be accessed on request by the general public in accordance with the FOIA.

The underlying principle is that all information held by a public authority should be freely available to the general public unless a valid exemption applies. The FOIA provides a right of access to non-personal information whereas the Data Protection Act 2018 gives individuals access to *personal* information about them that is held by organisations. Requests for access to environmental information are exempt under the FOIA and will be dealt with under the provisions of the Environmental Information Regulations 2004. The procedure for responding to such requests will follow that for responding to FOI requests.

The FOIA is fully retrospective and covers all information held by public bodies not only that obtained after the implementation of the FOIA.

The FOIA applies to all types of recorded information including:

- Financial;
- Corporate;
- Meeting papers and minutes
- Aims, targets and achievements
- Services offered
- Reports and independent enquiries
- Corporate policies and procedures
- Public involvement and

Under the FOIA anyone making a written request for information to the Practice is entitled to be informed in writing whether the information is held and, if so, to have it communicated to them. The person making the request does not need to mention the FOIA or state what they intend to do with the information. The Practice must respond to the applicant promptly and no later than 20 working days following the date of receipt. Requests for personal information must be handled within o under the provisions of the Data Protection Act.

For more information about your obligations under the FOIA, please visit this website:

https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

Appendix Two

Access to Health Records Policy

1. Introduction

The Access to Health Records Act 1990 gave individuals the right of access, subject to certain exceptions, to health information recorded about themselves, and, in certain circumstances, about others, within manual records. The Data Protection Act [DPA] 1998 came into force in March 2000 and repealed most of the 1990 Access to Health Records Act. All applications for access to records, whether paper based or electronic, of living persons are now made under the DPA.

For deceased persons, applications are made under sections of the 1990 Access to Health Records Act, which have been retained. These sections provide the right of access to the health records of deceased individuals for their personal representative and others having a claim under the estate of the deceased.

Under section seven of the DPA, patients have the right to apply for access to their health records. Provided that the fee has been paid and a written application is made by one of the individuals referred to below, the Practice is obliged to comply with a request for access subject to certain exceptions (see below). However, the Practice also has a duty to maintain the confidentiality of patient information and to satisfy itself that the applicant is entitled to have access before releasing information.

2. Applications

An application for access to health records may be made in any of the circumstances explained below.

2.1 *The Patient*

Prospect Surgery has a policy of openness with regard to health records and health professionals are encouraged to allow patients to access their health records on an informal basis. This should be recorded in the health record itself. The Department of Health's Code of Practice on Openness in the NHS as referred to in HSG (96) 18 Protection and Use of Patient Information will still apply to informal requests.

Such requests are usually made for a reason, and must always be in writing. There is no requirement to allow immediate access to a record of any type. The patient may have concerns about treatment that they have received, how they have been dealt with or may be worried that something they have said has been misinterpreted. All staff are encouraged to try to understand and allay any

underlying concerns that may have contributed to the request being made and offer an opportunity of early resolution.

2.2 *Children of 16 years or over*

2.2.1 If deemed to be "Gillick competent" a child is entitled to request or refuse access to their records. If any other individual requests access to these the practice should first check with the patient that he or she is happy for them to be released.

In all circumstances good practice dictates that a Gillick competent child should be encouraged to involve parents or other legal guardians in any treatment/disclosure decisions.

2.2.2 If the child is not deemed to be "Gillick competent" the individual[s] with parental responsibility for a child has a right to request access to those medical records. A person with parental responsibility is either:

i the birth mother, or
ii the birth father (if married to the mother at the time of child's birth or subsequently) or,
iii an individual given parental responsibility by a court.

2.3 *Patient Representatives*

A patient can give written authorisation for another person (for example a solicitor or relative) to make an application on their behalf. The Practice may withhold access if it is of the view that the patient authorising the access has not understood the meaning of the authorisation.

2.4 *Court Representatives*

A person appointed by the court to manage the affairs of a patient who is incapable of managing his or her own affairs may make an application. Access may be denied where the GP is of the opinion that the patient underwent relevant examinations or investigations in the expectation that the information would not be disclosed to the applicant.

2.5 *Access to a Deceased Patient's Medical Records*

Where the patient has died, the patient's personal representative or any person who may have a claim arising out of the patient's death may make an application. Access shall not be given (even to the personal representative) to any part of the record which, in the GP's opinion, would disclose information which is not relevant to any claim which may arise out of the patient's death.

The effect of this is that those requesting a deceased person's records should be asked to confirm the nature of the claim which they say they may have arising out of the person's death. If the person requesting the records was not the deceased's spouse or parent (where the deceased was unmarried) and if they were not a dependent of the deceased, it is unlikely that they will have a claim arising out of the death.

2.6 *Children and Family Court Advisory and Support Service (CAFCASS)*

Where CAFCASS has been appointed to write a report to advise a judge in relation to child welfare issues, Prospect Surgery would attempt to comply by providing factual information as requested.

Before records are disclosed, the patient or parent's consent (as set out above) should be obtained. If this is not possible, and in the absence of a court order, the Practice will need to balance its duty of confidentiality against the need for disclosure without consent where this is necessary:

i to protect the vital interests of the patient or others, or
ii to prevent or detect any unlawful act where disclosure is in the substantial public interest (eg serious crime), and
iii because seeking consent would prejudice those purposes.

The relevant health professional should provide factual information and their response should be forward to a member of the Child Protection Team who will approve the report.

2.7 *Chapter 8 Review*

All Chapter 8 Review requests for information should be immediately directed to the Primary Care Organisation Child Protection Manager who will co-ordinate the Chapter 8 Review in accordance with national and local Area Child Protection Committee Guidance.

3. Amendments to or Deletions from Records

If a patient feels information recorded on their health record is incorrect then they should firstly make an informal approach to the health professional concerned to discuss the situation in an attempt to have the records amended. If this avenue is unsuccessful then they may pursue a complaint under the NHS Complaints procedure in an attempt to have the information corrected or erased. The patient has a 'right' under the DPA to request that personal information contained within the medical records is rectified, blocked, erased or destroyed if this has been inaccurately recorded.

He or she may apply to the Information Commissioner but they could also apply for rectification through the courts. Prospect surgery, as the data controller, should take reasonable steps to ensure that the notes are accurate and if the patient believes these to be inaccurate, that this is noted in the records. Each situation will be decided upon the facts and the Practice will not be taken to have contravened the DPA if those reasonable steps were taken. In the normal course of events, however, it is most likely that these issues will be resolved amicably.

Further information can be obtained from the Commissioner at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, telephone number 01625 545700.

4. Other Requests

5.1 *Patients living abroad*

Former patients living outside of the UK and who once had treatment for their stay here, under the DPA 1998 they still have the same rights to apply for access to their UK health records. Such a request should be dealt with as someone making an access request from within the UK.

5.2 *Requests made by telephone*

No patient information may be disclosed to members of the public by telephone. However, it is sometimes necessary to give patient information to another NHS employee over the telephone. Before doing so, the identity of the person requesting the information must be confirmed. This may best be achieved by telephoning the person's official office and asking to be put through to their extension. Requests from patients must be made in writing.

5.3 *Requests made by the police*

In all cases the Practice can release confidential information if the patient has given his/her consent (preferably in writing) and understands the consequences of making that decision. There is, however, no legal obligation to disclose information to the police unless there is a court order or this is required under statute (e.g. Road Traffic Act).

The Practice does, however, have a power under the DPA and Crime Disorder Act to release confidential health records without consent for the purposes of the prevention or detection of crime or the apprehension or prosecution of offenders. The release of the information must be necessary for the administration of justice and is only lawful if this is necessary:

i to protect the patient or another person's vital interests, or
ii for the purposes of the prevention or detection of any unlawful act where seeking consent would prejudice those purposes and disclosure is in the

substantial public interest (e.g. where the seriousness of the crime means there is a pressing social need for disclosure).

Only information, which is strictly relevant to a specific police investigation, should be considered for release and only then if the police investigation would be seriously prejudiced or delayed without it. The police should be asked to provide written reasons why this information is relevant and essential for them to conclude their investigations.

5.4 *Court Proceedings*

A court of law may order the disclosure of all or part of the health record if it is relevant to a court case.

5. Application Process

6.1 GP Practices receive applications for access to records via a number of different sources, for example:

- Medical Insurance Companies
- Solicitors
- Patients
- Patient's carer
- Parents of children

Requests should be in writing, preferably on the application form at Appendix A. Where the request is not made by the patient, it must be accompanied by the patient's signed consent, and sufficient information to clearly identify the patient.

6.2 *Notification of requests*

Practices should treat all requests as potential claims for negligence. Good working practice would be to keep a central record of all requests in order to ensure that requests are cross-referenced with any complaints or incidents and that the deadlines for response are monitored and adhered to.

5.3 *Consideration of the application*

It is the GP's responsibility to consider an access request and to disclose the records if the correct procedure has been followed. Before the Practice discloses or provides copies of medical records the patient's GP must have been consulted and he/she checked the records and authorised the release, or part-release.

6.4 *Disclosure of the record*

Once the appropriate documentation has been received and disclosure approved, the copy of the health record may be sent to the patient or their representative in a sealed envelope by recorded delivery. The record should be sent to a named individual, marked confidential, for addressee only. Originals should not be sent.

Confidential information should never be sent by email unless via an encrypted service such as NHS Mail account to another NHS Mail account.

A note should be made in the file of what has been disclosed to whom and on what grounds.

Where information is not readily intelligible an explanation (e.g. of abbreviations or medical terminology) must be given.

6.5 *Refusing disclosure of the record*

The GP should refuse to disclose all or part of the health record if he/she is of the view that:

- disclosure would be likely to cause serious harm to the physical or mental health of the patient or any other person:
- the records refer to another individual who can be identified from that information (apart from a health professional). This is unless that other individual's consent is obtained or the records can be anonymised or it is reasonable in all the circumstances to comply with the request without that individual's consent, taking into account any duty of confidentiality owed to the third party; or if
- the request is being made for a child's records by someone with parental responsibility or for an incapacitated person's record by someone with power to manage their affairs, and the:
    - information was given by the patient in the expectation that it would not be disclosed to the person making the request, or
    - the patient has expressly indicated it should not be disclosed to that person.

6.6 *Informing of the decision not to disclose*

If a decision is taken that the record should not be disclosed, a letter must be sent by recorded delivery to the patient or their representative stating that disclosure would be likely to cause serious harm to the physical or mental health of the patient, or to any other person. The general position is that the Practice should inform the patient if records are to be withheld on the above basis. If however, the appropriate health professional thinks that telling the patient:

i will effectively amount to divulging that information, or this

ii is likely to cause serious physical or mental harm to the patient or another individual

then the GP could decide not to inform the patient, in which case an explanatory note should be made in the file.

The decision can only be taken by the GP and an explanatory note should be made in the file. Although there is no right of appeal to such a decision, it is the Practice's policy to give a patient the opportunity to have their case investigated by invoking the complaints procedure. The patient must be informed in writing that every assistance will be offered to them if they wish to do this. In addition, the patient may complain to the Information Commissioner for an independent ruling on whether non-disclosure is proper.

6.7 *Disclosure of a Deceased Patient's Medical Records*

The same procedure used for disclosing a living patient's records should be followed when there is a request for access to a deceased patient's records. Access should not be given if:

- the appropriate health professional is of the view that this information is likely to cause serious harm to the physical or mental health of any individual; or
- the records contain information relating to or provided by an individual (other than the patient or a health professional) who could be identified from that information (unless that individual has consented or can be anonymised): or
- the record contains a note made at the request of the patient before his/her death that he/she did not wish access to be given on application. (If while still alive, the patient asks for information about his/her right to restrict access after death, this should be provided together with an opportunity to express this wish in the notes.);
- the holder is of the opinion that the deceased person gave information or underwent investigations with the expectation that the information would not be disclosed to the applicant.
- the Practice considers that any part of the record is not relevant to any claim arising from the death of the patient.

6.8 *Timescales*

Copies of records should be supplied within 20 working days of receiving a valid and complete access request. In exceptional circumstances, it may take longer, with a maximum of 40 days. If this is to be the case, the patient must be advised prior to the expiry of the initial 20 working day period.

Where further information is required by the Practice to enable it to identify the record required or validate the request, this must be requested within 14 days of

receipt of the application and the timescale for responding begins on receipt of the full information.

6.9 *Charges*

There is no charge for record access. In instances where requests for copies of the same information are received or requests are deemed "unfounded, excessive or repetitive", a reasonable fee may be charged. However, this does not permit the organisation to charge for all subsequent access to records. on computer.

The Practice is not required to provide all the information requested if this would involve disproportionate effort. This however would only apply in very exceptional circumstances and may need to be justified to the Information Commissioner in the event of a dispute.

Resources

Access to Health Records: Department of Health - Policy and guidance

http://www.ico.gov.uk/for_organisations/freedom_of_information.aspx

Appendix A

APPLICATION FORM FOR ACCESS TO HEALTH RECORDS in accordance with the General Data Protection Regulations {GDPR} DATA SUBJECT ACCESS REQUEST {DSAR}

This form must be completed in blue or black ink and signed in order for us to process your request. You will be required to provide photographic proof of identity

Section 1 – Patient Details

Surname:		**Maiden Name:**	
First Name:		**Title: [Mr, Mrs, Miss, Ms, Dr**	
Date of Birth:		**Address:**	
Telephone Number:			
NHS Number: [if known]		**Postcode:**	

Details of the Person who wishes to access the records, if different to above:

Surname:	
First Name:	
Address:	
Telephone Number:	
Relationship to Patient:	

Declaration: I declare that the information given by me is correct to the best of my knowledge and that I am entitled to apply for access to the health records referred to above under the terms of the Data Protection Act 1998.

Section 2 – Record Requested

	Dates	Tick
Please provide me with a copy of test results, ie blood tests results, x-ray results etc.		
Please provide me with a copy of all records held		
Please provide me with a copy of records between dates specified		
Please provide me with a copy of records relating to the incident specified		
Please provide me with a copy of records relating to the condition		

Signature of Patient [if not the applicant]…….

Signature of Applicant…….

Date……
NOTES:

1. Under the Data Protection Act 1998 you do not have to give a reason for applying for access to your health records

2. 20 days notice is usually required

3. Please use the space below to inform us of any specific periods and parts of your health record you may require, or provide more information as requested above.

Appendix Three

Information Security Policy

1. Introduction

The purpose of the security policy is to ensure all employees are aware of the security procedures in place within the practice. All staff, are bound to comply with this policy.

2. Caldicott Guardian

A Caldicott Guardian is a senior member of staff appointed to overlook the management of Information Governance. The main priority of this role is to protect patient's information. Dr Sabir is the Caldicott Guardian for Prospect Surgery.

3. Purpose

1. To ensure that all staff are aware and fully comply with the relevant legislation as described in this policy.
2. To describe the principles of security and to explain how they shall be implemented at the practice.
3. To introduce a consistent approach to security and to ensure that all members of staff understand their own responsibilities.
4. To create and maintain within the practice a level of awareness of the need for Information Security as an integral part of the day to day business.

4. Scope

This information security policy applies to:

- All partners, employees and attached staff of the practice.
- All employees and agents of other organisations who directly or indirectly make use of or support the use of the computer system of this practice.

5. Responsibilities

Overall the Senior Partner assumes responsibility for information security and shall be the final authority on information security related matters

This Policy shall be maintained, reviewed and updated by the Practice Manager, on an annual basis.
Each user shall be responsible for the operational security of that part of the computer system, which they directly use. In addition attached staff shall be responsible for the security of the information, which they use, and/or share with others.

Each individual user of any part of the Practice's computer system has responsibility to comply with the security requirements which are in force to

ensure that the confidentiality, integrity and availability of the Practice's computer system is preserved to the highest standard.

Contracts with external organisations that access the Practice computer system should be in existence organisations shall comply with all appropriate security policies.

It is the responsibility of all staff to ensure they are working to the most up to date and relevant policies and procedures. By doing so, the quality of service offered will be maintained and the chances of information security and confidentiality being breeched will be minimised. All practice policies, protocols and guidance are stored securely at Prospect Surgery.

6. Keeping within the law

The Practice is obliged to abide by all relevant UK legislation and other relevant legislation from the European Union. This requirement devolves to the employees and agents of the Practice who may be held personally responsible for any breaches.

The Patients' Charter identifies "the right to have access to your health records" and the Data Protection Act (1984) and the Access to Health Records Act (1990), with some exceptions, entitles individuals to a copy of computerised information held about them. Patients do not have to give reasons for seeking advice. N.B. There is specific guidance on access to records sought in connection with legal proceedings.

6.1 The Copyright, Designs and Patents Act 1988

All computer software used on the Practice's system must be properly licensed. The Practice may be prosecuted if illegally copied software is found to be resident on any of the information systems in use by the Practice.

Prospect Surgery will be responsible for conducting software audits annually to ensure that all software has been properly procured and licensed.

No member of staff or attached staff should copy software illegally, nor introduce illegally copied or any other unauthorised software into any part of the Practices' Computer System, nor knowingly use illegally copied software. Any person who does shall be subject, upon discovery, to severe disciplinary action.

6.2 The Computer Misuse Act (1990)

The purpose of this legislation is to ease the prosecution of persons who access systems when they are unauthorised to do so.

6.3 **Health and Safety at Work Act (1974)**

Computers should be used in a manner that does not affect the user's health. This is verified by annual risk assessments, where appropriate.

7. **Personal Security**

All staff have signed a contract of employment with the Practice. This includes reference to the need to maintain a high standard of confidentiality. Disclosure or misuse of personal data will be treated as a serious disciplinary offence, which may result in dismissal**.**

The Practice always take up the personal and previous work references of all new employees.

It is the responsibility of each member of staff to be aware of the full nature of their responsibilities and in particular the limits of those responsibilities. To achieve this all members of staff have a current written job description.

It is the intention of the Practice that all members of staff should receive appropriate training to enable them to carry out their work efficiently. It is the responsibility of the Assistant Practice Manager/Senior Receptionist, in conjunction with the users themselves, to ensure that everyone who uses the computer system is competent to do so, appreciates the importance of providing correct information and fully understands the status of the output received.

In order to support an efficient and knowledgeable working practice, each member of staff shall have access to appropriate documentation. However, it is recognised that such documentation may also be of help to someone who may wish to attempt to gain unauthorised access to the system, and it should, therefore be held securely at all times.

If each user becomes aware of errors, which apparently have been made by the System, themselves or colleagues, it is important that they report these to the Assistant Practice Manager/Senior Receptionist. The seriousness of the error is not the main issue. Even minor errors should be notified as they may be symptomatic of a deeper and much more serious issue.

8. Technical Security

All reasonable efforts shall be made to ensure that the system software controls those who are allowed to access the system.

Each user is allocated a unique user identity, which shall be used during the log on process to validate a genuine user, and track system use. The user can use this identity to record all subsequent actions.

Each user of the system chooses a unique password. All passwords must be at least six characters long and are kept secret for the individual's use. These passwords are changed every two months.

Each member of staff is given access only to information relevant to their workload. The Practice or Deputy Manager determines the authorisation to be given to each member of staff and reviews this access at regular intervals.

Dr Sabir, the Practice Manager and Deputy Manager have full admin access rights. In order to ensure information is protected, the random audits, such as the following, may be undertaken:

- a selection of random patient's computer records
- staff access to the computer system (smart card audit trail)
- Record of telephone calls

9. Back up procedures

The Clinical System used by the practice is SystmOne, and back-ups for this system are undertaken off-site by the service provider, TPP.

Other back-up processes are covered in the practice Business Continuity Plan.

10. Data disposal

All sensitive material should be cleared off hard disks and floppies before disposal, in accordance with the IM & T Security Manual.

All incoming correspondence is scanned on to the clinical system within 48 hours. The original documentation is then shredded 1 week later.

All confidential waste is shredded.

11. Security administration

The Practice Manager is responsible for the security of the Practice's computer network. This does not mean that she should carry out all the tasks directly but shall be responsible for ensuring that they are carried out and that they are carried out efficiently and effectively. In general she will be responsible for:

- The continued availability of data to each-user when and where it is needed.
- The preservation of the confidentiality of all data on the system
- The development of initial security policies which reflect the security needs of the system

and is required to: -

- Monitor the effectiveness of the security policy
- Monitor compliance of staff with security procedures through observation and evidence of computer generated records
- Maintain the level of protection to an adequate level by acting on the evidence provided from the monitoring procedure
- Provide security education for all users of the system
- Reassess whether the security measures are still relevant to the current threats to the system
- Reassess whether the security policies are still adequate
- Monitor new systems

A fundamental prerequisite for the development of new or additional security is the carrying out of a risk analysis exercise. This should be done whether the new security is to improve the security of an existing system or whether it is to be part of the design of a new system or major enhancement. Finance for implementing protective measures shall not be expended unless they can be justified.

12. Data transmission

The number of attempts to access the network shall be restricted.

User authorisation records shall be examined regularly to ensure compliance. The record of people, both staff and others, who are authorised users, shall be made inactive immediately when their authorisation becomes invalid e.g. on leaving the Practice's employment or on amendment of privileges.

Internal

All physical connections to the practice network must be authorised by the Practice or Deputy Manager. Users must not connect unauthorised hardware to the practice network.

All network equipment shall be allocated a unique serial number and inspections made to ensure that only authorised equipment is connected to the network. All serial numbers are included in inventory.

External

Access granted to system suppliers (TPP) through firewall for the purpose of updates through BT Integra.

13. Procurement

New software, which has not been properly developed and/or properly tested, is a threat to the security of existing data. The Practice will work with the CCG/TPP to ensure that all software procurements take into account security requirements.

14. Web browsing

Accessing illegal sites and/or transmitting data over the NHS net are not permissible and will result in disciplinary action being taken. Non-work related sites should only be visited with prior permission from the Practice or Deputy Manager.

15. Security

Sophos netshield anti virus software is installed on all pc's, which are networked to the Internet. This is automatically updated every week from ftp.nai.com/virusdefs/4.x.

16. Email use

This is a useful tool if not abused and used correctly, but can be time wasting and an annoyance if used inappropriately. E-mail use is strictly restricted to work use only. External emails can only be sent with prior permission from the Practice or Deputy Manager. Mass unsolicited emails will not be tolerated. Disregard of these guidelines may result in disciplinary action being taken as outlined in staff contracts.

N.B. Risk can never be eliminated; the objective is to reduce the risk to a level, which is considered to be acceptable.

17. Working from home

Any staff member wishing to work from home/from another site/outside of normal contractual hours must be granted permission to do so by the Practice or Deputy Manager. This is to ensure that the clinical system is only accessed by authorised personnel in an environment which is secure.

If and when permission is granted, conditions of this arrangement will be made in writing to the home worker. These conditions will ensure the security of data off site, paying particular attention to the security arrangements in transporting information to and from the place of work and the security of information in the home.

18. References

First Practice Management Policies and Procedures Library, (www.firstpracticemanagement.co.uk).

Appendix Four

Policy and Protocol for Record Keeping and the Storage, Retention and Destruction of Health Records

1. Introduction

Record keeping is a tool of professional practice and one that should help the care process. It is not separate from this process and it is not an optional extra to be fitted in if circumstances allow.

Staff working within Prospect Surgery must ensure that their record keeping fulfils all legal and contractual requirements, as well as professional guidelines. Accurate record keeping helps protect staff, patients/clients and the practice in the event of litigation.

The quality of record keeping is a reflection of the standard of an individual's professional practice. Good record keeping is a mark of the skilled and safe practitioner, whilst careless or incomplete record keeping often highlights wider problems with an individual's practice.

This policy should be read in conjunction with the NHS Code of Confidentiality Policy.

2. What is a record?

In the context of this policy, a record is anything, which contains information (in any media), which has been created or gathered as a result of the work of practice employees and attached staff – including locums, agency or casual staff.

3. Accountability and Responsibility

This policy applies to:

- All partners, employees and attached staff of the practice.
- All employees and agents of other organisations who directly or indirectly make use of or support the use of the computer system of this practice.

The Partners are personally accountable for the quality of records management within the Practice.

All line managers and supervisors must ensure that their staff are adequately trained and apply the appropriate guidelines.

Where computerised records are used, authorised personnel should have received appropriate training for safe and secure use of the system.
In practice, individual members of staff are responsible for any records, which they create or use. This responsibility is established at, and defined by, the law.

4. Legal Issues

The NHS and all persons working within the NHS have a common law duty to patients and a duty to maintain professional, ethical standards of confidentiality. This means everyone working within the Practice has a personal common law duty of confidence to patients and to the Practice. The duty of confidence continues after the patient has died and/or the employee has left the Practice. Patient records must not be accessed by health professionals or other authorised staff, other than by those who are directly involved in the patient's care.

In the event that patient's records are required for clinical audit explicit consent may not be necessary as the current and subsequent care to the patient will not be affected. Health professionals and other authorised staff may have access to records with the inference that they follow Practice policy and the Data Protection Act with regard to confidentiality. Results presented as part of a report or presentation must not contain any patient identifiable information (patient name, patient ID, NHS number, date of birth etc).

5. Content and Style of Paper-Based Records

All entries must be **legible** and written in **ink**.
All entries must be preceded by:

- the date and time at which they are written

They must also be:

- Factual
- Objective
- In chronological order

The professional formulating the plan of care must:

- Print their name
- Sign at the end
- State their professional qualification

Best practice dictates that records should be completed at the time of the intervention. However, where this is not possible, retrospective entries **must** be recorded within 24 hours of patient/ client contact.

All entries must:

- Be signed at the time of writing
- Have each name printed after signature at least once within the record.
- If there are any spaces between entries and/or entry and signature, this space must be scored with a single line.
- Abbreviations should be avoided where possible. Where an abbreviation is used the practitioner must ensure this is not ambiguous and there is evidence

of its meaning within the record. An abbreviations list has been developed shown in Appendix 1.

- The patient's name, date of birth and NHS number must be documented on each sheet of their record.
- Individual records must not be tagged/coded for recognition purposes.
- Summary significant event sheets must be used rather than the use of highlighter pens.
- Ditto lines must not be used.

All assessments must be comprehensive and where relevant include the following needs:

- Physical
- Social
- Mental health
- Communication
- Cultural
- Spiritual
- Carers involvement
- Care plans
- Review date identified by each professional
- If relevant, documentation must reflect multi-disciplinary/agency care.

Where it is necessary to create a continuation record:

- All documentation must be kept together
- It must be made clear which documentation is currently in use.

6. Alterations of Paper-Based Records

The original entry must not be erased but be scored by a single line, followed by:

- Signature of person altering the record
- Date
- Time

7. Electronic Patient Records

The principles of good records management practice described in this policy apply equally to records created electronically.

It is never acceptable for an entry to be made into a record using another users login details. It is essential that all users:

- Have a unique user identity and password
- Keep their password secret and do not divulge it to other users for any reason.
- Change their password at frequent intervals
- Log out of workstations when their task at that workstation is finished.

- Never leave a workstation logged in but unattended.

It is already a matter of professional and public policy that general practice (and all NHS Electronic Patient Record systems) should use a common coding scheme so that health professionals may share and have a common understanding of medical information. It is never acceptable to use free text to modify the fundamental meaning of a coded entry.

8. Transportation of Records

Patient records must remain in the practice (or patient's home in the case of patient held records) unless absolutely necessary. When removed from the practice they must be recorded as being removed and returned promptly.

If practitioners need to transport records in their vehicle they must be kept out of sight in a locked boot.

Patient records must not be left in vehicles overnight.

Prospect Surgery uses the clinical system SystmOne. Therefore, when a patient registers with another SystmOne surgery the record is automatically accessible to that practice.

Where a patient transfers to a non-SystmOne surgery the information in his or her "current" computerised patient record must be sent to the new practice. The record is first returned to the Strategic Health Authority in the sealed internal mail bag, who will forward to the new practice in due course. Otherwise a printed copy of all the electronic record must be sent.

9. Storage of Records

Each record should have a unique identifier[1] that allows it to be readily retrieved from storage if required.

Records must always be kept securely and when a room containing records is left unattended, it should be locked. A sensible balance should be achieved between the needs for security and accessibility.

The conditions in which paper records are kept should be free from any risk of fire or flooding. If there were to be a risk associated with the storage arrangement of health records, a risk assessment would be required by the Practice Manager to allow remedial action to be taken.

Systems for electronic records should be designed so that records will remain accessible, authentic, reliable and usable through any kind of system change, for the entire period of retention. This may include migration to different software, re-presentation in emulation formats or any other future ways of re-presenting

records. Where such processes occur, evidence of these should be kept, along with details of any variation in records design and format.

There should also exist, suitable measures to physically secure computerised records. These measures include: Uninterruptible Power Supplies (UPS), a fire safe for the local holding of back-up and other sensitive removable media and additional security measures such as desk chains, lockable boxes for main processing unit(s) and movement alarms.

As the need for quick access to particular records reduces, it may be more efficient to move less frequently used records off site.

Off-site storage can be especially beneficial for less frequently used material, and private sector companies are capable of providing secure and efficient information storage and retrieval services for all types of record.

10. Retention of Health Records

To follow is a summary of the retention periods for records, which are not for permanent preservation, or which are no longer required for their original purpose. *Minimum retention periods should be calculated from the end of the calendar year.*

10.1 *Records*

The recommended minimum retention periods apply to both paper-based and computerised records though extra care needs to be taken to prevent corruption or deterioration of the data. Re-recording/migration of data will also need to be considered as equipment and software become obsolete. Computerised records of patients who are no longer registered should be made inactive or archived.

10.2 *Patient Health Records*

The retention periods listed below reflect minimum requirements of clinical need. Personal health records may be required as evidence in legal actions; the minimum retention periods take account of this requirement.

Pre 1948 records	Should have been transferred for permanent preservation or destroyed. Any pre-1948 records, which still exist, should be considered for permanent preservation. For advice on this please contact the Data Protection Officer who will liaise with the Public Records Office.

Children and young people	Until the patient's 25th birthday, or 26th if the person was 17 at conclusion of treatment; or 8 years after the patient's death if death occurred before the patient's 18th birthday
Records relating to those serving HM Armed Forces	Should not be destroyed
Records relating to those serving a prison sentence	Should not be destroyed
Donor records	11 years post transplantation
Maternity	(all obstetric and midwifery records including those of episodes of maternity care that end in still birth or where the child later dies) – 25 years
Mentally disordered persons	(within the meaning of the Mental Health Act 1983) – 20 years after no further treatment is considered necessary; or 8 years after the patient's death if patient died while receiving treatment
Oncology	8 years after conclusion of treatment, especially when surgery only involved
Patients involved in clinical trials	15 years after conclusion of treatment
Xray films and reports	retain x-ray films for a period of 5 years and the corresponding reports for 8 years.
General	(anything not covered above) – 8 years after conclusion of treatment.
Any individual records identified by clinical staff as DO NOT DESTROY	until the date specified by the clinician
All other personal health records	10 years after conclusion of treatment, the patient's death or after the patient has permanently left the country

.

This takes account of legal requirements and sets out the **minimum** retention periods for both clinical and administrative records. You do, however, have local discretion to keep material for longer, subject to local needs.

Where a record is not referred to above, advice must be sought from the Practice Manager.

11. Disposal

Under normal circumstances all records will be destroyed as soon as is practicable after the expiry of the relevant minimum retention period.

Other options for disposal include transferring the record to another medium (e.g. computer) or another use (e.g. Public Records Office). The Public Records Office in this area is at: Teesside Archives, Exchange House, 6 Marton Road, Middlesbrough, TS1 1DB Tel: 01642 248321.

It is vital that confidentiality is safeguarded at every stage and that the method used to destroy such records is fully effective and secures their complete illegibility. Normally this will involve shredding, pulping or incineration.

The following principles should govern the physical destruction of records:

- Destruction should always be authorised
- Records pertaining to pending or actual litigation or investigation should not be destroyed
- Authorised records destruction should be carried out in a way that preserves the confidentiality of any information they contain.
- All copies that are authorised for destruction, including security copies, preservation copies and back-up copies should be destroyed.

12. Key Documents

- Guidelines for Records and Record Keeping *Nursing & Midwifery Council* (2002)
- Essence of Care Modernisation *Agency* (2002)
- For the record: managing records in NHS Trusts and Health Authorities Health *Service Circular HSC 1999/053* (1999)
- Preservation, Retention and Destruction of GP General Medical Services Records Relating to Patients NHS *Executive Health Service Circular* (1998)
- Good Practice Guidelines for General Practice EPR NHS *Executive* (2000)
- HMSO Data Protection Act 1998 London HMSO
- Audit Commission 1999 A First Class Service: quality in the NHS, Department of Health

Information – retention periods

These are suggested retention periods for documentation. The list is endless; however, the ones which relate to general practice are listed below.

Record Type	Retention period (years)	Notes
Abortion certificate (HSA1)	3	Abortion regulations. 1991
Accident Register (RIDDOR)	3	Reporting of injuries, diseases and dangerous occurrences
Accounts – Annual (final)	Permanent	
Accounts – Costs	3	
Accounts – Financial	7	
Audit Records – original documentation	2	From completion of the audit
Buildings – papers relating to occupation (but not health and safety information)	3	After occupation ceases. Construction & design management regulations 1994
Buildings and engineering works, inclusive of major projects abandoned or deferred - key records, (e.g. Final accounts, surveys, site plans, bills of quantities)	Permanent	
Buildings and engineering works, inclusive of major projects abandoned or deferred - town and country planning matters and all formal contract documents (e.g. Executed agreements, conditions of contract, specifications, "as built" record drawing and documents on the appointment and conditions of engagement of private buildings and engineering consultants.	Life of building and installations to which they refer	
Complaints records	10	

Record Type	Retention period (years)	Notes
Computerised records		The recommended minimum retention periods apply to both paper and computerised records, though extra care needs to be taken to prevent corruption or deterioration of the data. Re-recording/migration of data will also need to be considered as equipment and software become obsolete.
Contracts – on termination	6	The Limitation Act, 1980
Death certificate counterfoils	6 months	Unless there is a query (i.e. the death has been referred to the coroner)
Delivery notes	1.5	
Diaries – office – on completion	1	
Establishment records – major (e.g. Personal files, letters of appointment, contract references)	6	Keep for 6 years after subject of file leaves service or until subject's 70th birthday, whichever is the later.
Establishment records – minor (e.g. attendance books, annual leave records, timesheets	2	
Freedom of Information Requests	3 years after full disclosure, 10 years if information is redacted or the information requested is not disclosed.	
Health and safety documentation	3 years	
Invoices	6	The Limitation Act 1980
Job Advertisements	1	
Job Descriptions	3	Following termination of employment
Meeting papers - committees, sub-committees (Master copies)	10	
Minutes – reference copies	10	

Record Type	Retention period (years)	Notes
Nurses Training Records	30	
Papers of minor or short-lived importance not covered elsewhere, eg: advertising matter, covering letters, reminder Letters, anonymous or unintelligible letters, drafts, duplicates of documents known to be preserved elsewhere (unless they have important minutes on them), indices and registers compiled for temporary purposes, routine reports punched cards, other documents that have ceased to be of value on settlement of the matter involved	2 years after the settlement of the matter to which they relate.	
Patient Group Directives (Nursing PGD's)	Retain as long as clinical records – in the event of challenge	"A PGD is documentation of how the nurse practiced over the period of time the PGD was in use. Therefore a record of the PGD should be kept as long as other records are kept in case clinical practice is challenged. The practice needs to keep a copy of the PGD rather than the specific PGD the nurse signed. However the practice should keep a record of the fact that the nurse signed up to the PGD. The PCT also keep copies of archived PGD's.
Patient record – adult	Return to HA	20 years after no further treatment considered necessary; or 8 years after death. Suicide records will be retained permanently, as classed as serious incident.

Record Type	Retention period (years)	Notes
Patient record – child	Return to HA	Until the patient's 26th birthday, unless treatment being received then in line with adult record; or 8 years after patients' death. Suicide records will be retained permanently, as classed as serious incident.
Pay roll – full-time medical staff	6	For superannuation purposes
Pay roll – other staff	6	
PAYE records	6	
Policy and procedures (administrative and clinical, strategy documents)	10 years after life of the system (or suspended) to which the policies or procedures refer	
Records – Major incidents	Permanent	
Receipt for registered and recorded delivery mail	2 years	Following the end of the financial year to which they relate
Recruitment documents	3	Information on successful candidate should be retained with staff personnel file
Registration/Maternity forms (item of service style)	3	As per advice from registrations department
Request for access to records, other that Freedom of Information or subject access requests	6 years after last action	
Wages/Salaries	10	For superannuation purposes