Polaris Medical: Data Protection Policy

Policy Category	Ethics, Integrity and Legal
Author	Alexander Davidson
Position	Information and Compliance Officer
Reviewed by	Lee Major
Position	Operations Director
Approved by	Norman Henderson
Position	Managing Director
Signature	
Date of Issue	Sept 2018
Review Date	Sept 2020
Version	1.1

Contents


CYBER
ESSENTIALS
PLUS
Regulated by
CareQuality
Commission

1. Introduction

Polaris Medical needs to collect and use information about people to carry out its business activities and fulfil statutory obligations.

The information is held on past, current, and prospective patients, employees, clients/customers, suppliers, and others with whom we communicate. Some information may have to be collected to satisfy our legal obligations.

Personal information must be handled properly no matter how it is collected, recorded, used, or disseminated: on paper, in a computer, or recorded in other ways.

Polaris Medical is required to comply with all relevant UK and European Union legislation. This obligation extends to employees and agents of the company who may be personally liable, as well as the company, for any breaches.

In addition, the Government's commitment to implement the recommendations of the Caldicott Committee requires every NHS organisation and independent health organisation to have a Caldicott Guardian to ensure the protection and use of confidential patient information. There is an on-going programme to improve the use and safekeeping of patient identifiable information within the company. The company Caldicott Guardian is the Administration and Compliance officer.

As well as the common law duty of confidentiality that prohibits use or disclosure of personal information given in confidence, all staff must adhere to the seven Caldicott principles (Caldicott Report 1997 and Review of 2013).

2. Scope

This policy applies to all Polaris Medical staff and patients.

3. Policy Statement

This policy aims to ensure that:

- There is a nominated person with specific responsibility for data protection
- Everyone managing and handling personal information:
    - understands s/he is contractually responsible for following good data protection practice
    - is appropriately trained to do so; and is appropriately supervised
- Anyone wanting to make enquiries about handling personal information knows what to do
- Clear procedures on handling personal information:
    - are in place and
    - are regularly assessed and evaluated
- Performance with handling personal information is regularly assessed and evaluated

Policy

4. Data Protection Principles

Objective

To ensure anyone processing Personal Data within Polaris Medical complies with the eight enforceable principles of good practice.

Data Protection Principles

The Act requires that personal data:

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met, and in the case of sensitive personal data, an additional condition is also met
2. Shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. Shall be accurate and, where necessary, kept up to date
5. Shall not be kept for longer than is necessary for that purpose or those purposes
6. Processed in accordance with the rights of data subjects under the Act; and that:
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

5. Caldicott Principles

Objective

To ensure anyone processing personal data within Polaris Medical applies the seven general principles of good practice in handling patient-identifiable information.

Caldicott Principles

Access to person identifiable information should be restricted to those staff who have a justifiable need to know in order to carry out their jobs effectively. The Caldicott Principles underpin the approach that Health Care organisation should develop and introduce at a pace that is sustainable locally:

1. Justify the purpose(s)

Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian

2. Don't use patient-identifiable information unless it is absolutely necessary

Patient-identifiable information items should not be used unless there is no alternative

3. Use the minimum necessary patient-identifiable information

Where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiability

4. Access to patient-identifiable information should be on a strict need to know basis

Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see

5. Everyone should be aware of their responsibilities

Action should be taken to ensure that those handling patient- identifiable information - both clinical and non-clinical staff - are aware of their responsibilities and obligations to respect patient confidentiality

6. Understand and comply with the law

Every use of patient-identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.

7. The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies

6. Organisational Management

Objective

To establish the management structure for good practice to manage data effectively and respect personal privacy within Polaris Medical.

Management Responsibilities

Polaris Medical will, by strict application of criteria and controls:

- Fully observe conditions for the fair collection and use of information
- Meet its legal obligations to specify the purposes for which information is used
- Collect and process relevant information, and only to the extent it is needed to fulfill operational needs or to comply with legal requirements
- Ensure the quality of information used
- Apply strict checks to determine how long information is held
- Ensure people whose information is held can fully exercise their rights under the DPA 1998
- Take appropriate technical and organisational security measures to safeguard personal information
- Ensure personal information is not transferred outside the EEC without suitable safeguards.
- There is a nominated person, the Data Protection Officer, with specific responsibility for data protection
- There is a nominated person, the Caldicott Guardian, with specific responsibility for internal protocols governing access to patient-identifiable information
- Everyone managing and handling personal information is aware of their responsibilities;
- Anyone wanting to make enquiries about handling personal information knows what to do;
- Clear procedures on handling personal information;
    - are in place
    - are regularly assessed and evaluated; and
    - the performance of these procedures is regularly monitored and evaluated

Data Protection Officer

The Data Protection Officer for the company is the Director of Finance and Information Technology. He/she:

- Must ensure appropriate Data Protection Act notification is maintained for the organisation's systems and information
- Is responsible for dealing with enquiries about the Data Protection Act, and facilitating Subject Access requests
- Is responsible for advising users of their responsibilities under the Data Protection Act, including Subject Access
- Is responsible for advising the Administration and Compliance Officer on breaches of the Act, and recommending actions
- Is responsible for liaising with external organisations on Data Protection Act matters.

Caldicott Guardian

The Caldicott Guardian for the company is the Director of Patient Care. He/she is responsible for:

- Agreeing, monitoring, and reviewing internal protocols governing access to personally- identifiable information by staff within the organisation, in compliance with UK legislation and national policy and guidance;
- Agreeing, monitoring, and reviewing protocols governing the use of personally-identifiable information across organisations, e.g. with NHS and local authority services, and other partner organisations contributing to the local provision of care.

Staff Responsibilities

Everyone managing and handling personal information:

- Understands s/he is contractually responsible for following good data protection practice
- Is aware of her/his responsibilities and obligations to respect patient confidentiality
- Is appropriately trained to do so
- Is appropriately supervised

Staff are also legally liable if they breach legislation relating to gathering, storage or processing of data at all times.

7. Access Requests

Access to Health Records

A 'health record' is defined in DPA 1998 as: *any record which consists of information relating to the physical or mental health or condition of an individual, and has been made by or on behalf of a health professional in connection with the care of that individual*.

The definition can include material held in other media: an X-ray, MRI scan, or video, for example. This means that when a subject access request is made, the information contained in such material must be supplied to the applicant within the fee charged.

Most of the records held by companies, surgeries and other health care institutions are 'health records' and therefore fall within the scope of the 1998 DPA's subject access provisions.

Dealing with Subject Access Requests and Requests for Information from Third parties

A formal request from a data subject for information that we hold about them personally must be made in writing. A fee is payable by the data subject for provision of this information. Any member of staff who receives a written request should forward it to their line manager immediately. If the line manager is not available or unclear on how to act the line manager should contact the Data Protection Compliance Officer. Further guidance is available here: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/

In the case of **requests from individuals** about their own information, the individual is entitled to be:

- told whether any personal data is being processed
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people
- given a copy of the information comprising the data

- given details of the source of the data (where this is available)
- receive the response to their request within 40 calendar days of us receiving it

Note: A request is valid even if the individual has not sent it directly to the person who normally deals with such requests – so it is important to ensure that you can recognise a subject access request and handle it appropriately.

When handling **requests from third parties/organisations** that relate to another individual's information, The Act recognises that it is sometimes appropriate to disclose personal data for the certain purposes of the prevention or detection of crime, the capture or prosecution of offenders and the assessment or collection of tax or duty. Under the Act these are known as exemptions.

The police are most likely to ask you to release personal information under this exemption. However, you may get requests from other organisations that can rely upon this exemption because they have a crime prevention or law enforcement function, for example, the Department for Work and Pensions – Benefit Fraud Section.

These exemptions do not cover the disclosure of all personal information, in all circumstances. It only allows you to release personal information for the stated purposes and only if not releasing it would be likely to prejudice (that is, significantly harm) any attempt by the requestor (for example, the police) to prevent crime or catch a suspect.

Contact the Data Protection Compliance Officer where you receive a request from any third party relating to another individual's information, ask them to put the request in writing, outlining the importance of why they require the information (bearing in mind the type of information being requested and the extent of it), and what would be the consequences if we failed to provide it. Once you have received this information from the requestor, please contact the Data Protection Compliance Officer for information on how to proceed.

Never feel obliged to provide information without first being given the opportunity to consult with the Data Protection/Information and Compliance Manager. These exemptions do not require you to disclose personal data to the police or to other law enforcement agencies – they merely keep you within the Data Protection Act if you decide to disclose information in the circumstances in which the exemptions apply. It is for this reason that we must handle any requests from third parties very carefully.

If you have any doubts regarding obligations under the Act, please contact the Data Protection/ Information and Compliance Manager.

In general, the right of subject access allows an individual to gain access to her/his personal data however it is held and whenever it was made.

This normally involves providing an individual with copies of her/his records when asked to do so.

You must also give the data subject:

- A description of the data
- A description of the purpose/s for which the data are being or are to be processed
- A description of those to whom the data are disclosed

In addition, you must give the data subject:

- Any information available to the controller about the source of the data
- An explanation of any automated decision taken about the data subject

Exceptions to Subject Access

Apart from where the appropriate fee has not been paid, the main exceptions are:

- Information processed for scientific research where the results cannot identify the person
- Where disclosing the personal data would reveal information about someone else unless they have consented to the disclosure, or would be expected to
- Information about their physical or mental health or condition: Where permitting access would be likely to cause serious harm to the physical or mental health or condition of the data subject or another person
- Where the request is made by another, such as a parent for a child on behalf of the data subject, access can be refused if the data subject had either provided the information in the expectation it would not be disclosed, or had indicated it should not be, to the applicant; or if the data was obtained as a result of an examination or investigation to which the data subject consented on the basis that information would not be so disclosed.

8. Safe Haven

The term **safe haven** is a location (or in some cases a piece of equipment) situated on The Company's premises where arrangements and procedures are in place to ensure person-identifiable information can be held, received and communicated securely.

Where safe haven procedures should be in place

Safe haven procedures should be in place in any location where large amounts of personal information is being received, held or communicated especially where the personal information is of a sensitive nature. There should be at least one area designated as a safe haven at each of The Company's sites.

Responsibilities for Implementing the Safe Haven Policy

The Caldicott Guidelines are adopted by The Company & must approve all procedures that relate to the use of patient information.

The **HR Manager** is responsible for coordinating improvements in: data protection, the confidentiality code of conduct and with the Director of IM&T on information security.

All staff that process personal-identifiable information and Managers who have responsibilities for those staff must adhere to this policy.

Requirements for safe havens

Location/security arrangements:

- It should be a room that is locked or accessible via key pad known only to authorised staff or
- The office or workspace should be sited in such a way that only authorised staff can enter that location i.e. it is not an area which is readily accessible to any member of staff who work in the same building or office, or any visitors.
- If sited on the ground floor any windows should have locks on them.
- The room should conform to health and safety requirements in terms of fire, safety from flood, theft or environmental damage.
- Manual paper records contained person-identifiable information should be stored in locked cabinets.
- Computers should be not left on view or accessible to unauthorised staff and have a secure screen saver function and be switched off when not in use.
- Equipment such as fax machines/ Telephones in the safe haven should have a code password and be turned off out of office hours.

Communications by post

- All sensitive records must be stored face down in public areas and not left unsupervised at any time
- Incoming mail should be opened away from public areas
- Outgoing mail (both internal and external) should be sealed securely and marked private and confidential

Computers

- Access to any PC must be password protected, this must not be shared.
- Computer screens must not be left on view so members of the general public or staff who do not have a justified need to view the information can see personal data.
- PCs or laptops not in use should be switched off or have a secure screen saver device in use.
- Information should be held on the Organization's network servers, not stored on local hard drives. Offices should be aware of the high risk of storing information locally and take appropriate security measures.
- All personal information sent by e-mail should be password protected
- Clinical information must be clearly marked and checked by the Clinical Supervisor.
- Emails must be sent to the right people, check and double check addresses
- Browsers are safely set up so that for example, passwords are not saved and temporary internet files are deleted on exit

- The receiver is ready to handle the information in the right way
- Information sent by email will be safely stored and archived as well as being incorporated into patient records
- There is an audit trail to show who did what and when
- There are adequate fall back and fail-safe arrangements
- Information is not saved or copied into any PC or media that is “outside Polaris Medical”
- Great care should be taken in sending personal information especially where the information maybe of a clinical nature – it should be password protected and procedures undertaken to ensure that the correct person has received it.

Sharing information with other Organizations (Non NHS)

Employees/ Sub Contractors of The Company authorised to disclose information to other organisations like that of the NHS must seek an assurance that these organisations have a designated safe haven point for receiving personal information. The Company must be assured that these organisations are able to comply with the safe haven ethos and meet certain legislative and related guidance requirements:

- Data Protection Act 1998
- Common Law Duty of Confidence
- Code of Practice: Confidentiality

Staff sharing personal information with other agencies should be aware of protocol agreements made with other agencies, for example Police Forces, Social Services

All of these documents are available on Polaris Medical Intranet pages & in all office locations.

9. Monitoring and Review

This policy will be reviewed every 2 years.

10. Links to Other Company Policies and Procedures

Code of Confidentiality

Confidentiality Policy

Information Quality and Records Management Policy

Records Retention Policy

IT Security Policy

References:

Health and Social Services Guidance

- Ensuring Security and Confidentiality in NHS Organisations. (E5498).
- The Records Management: NHS Code of Practice
- Health Service Circular (HSC 2000/009) - Protection and Use of Patient Information
- Health Service Guidance (HSG (96) 18) - The Protection and Use of Patient Information

Legislation

- Access to Health Records Act 1990
- Access to Medical Reports Act 1988
- Childrens Act 2004
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Crime & Disorder Act 1998
- Data Protection Act 1998
- Communications Act 2003
- Freedom of Information Act 2000
- Health and Social Care Act 2012
- Human Rights Act 1998
- Police and Criminal Evidence Act 1984
- Public Records Act 1967
- Regulation of Investigatory Powers Act 2000
- Environmental Information Regulations 2004

Appendix 1: Glossary

For the purposes of this policy the following definitions apply.

A **Health Professional** is any of the following:

a) a registered medical practitioner
b) a registered dentist
c) a registered optician
d) a registered pharmaceutical chemist
e) a registered nurse
f) a registered osteopath
g) a registered chiropractor
h) any person who is registered as a member of a profession to which the Professions Supplementary to Medicine Act 1960 for the time being extends
i) a clinical psychologist, child psychotherapist or speech therapist,
j) a music therapist employed by a health service body, or
k) a scientist employed by such a body as head of a department [DPA 1998 S69]
l) Ambulance Paramedic
m) Ambulance Technician
n) Ambulance Care Assistant

A **Health Record** is any record which consists of information relating to the physical or mental health or condition of an individual made by or on behalf of a health professional in connection with the care of that individual. [DPA 1998 S68(2)]

An **Information Commissioner** is a person appointed by Government to administer the provisions of the DPA and FOI. Before FOI, called the Data Protection Registrar (1984) or the Data Protection Commissioner (1998)

Medical purposes includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services [DPA 1998]

NHS organisations: All organisations providing healthcare services, including strategic health authorities, special health authorities, primary care companies, NHS companies, general medical and dental practices

Password: Confidential authentication information composed of a string of characters

Personal data: data which relates to a living individual who can be identified

a) from that data; or
b) from that and other information in the possession of, or likely to come in the possession of, the Data Controller; and
c) includes any expression of opinion about the individual and any other indication of the intentions of the Data Controller or any other person in respect of the individual

[DPA 1998]

Processing (in obtaining, recording or holding the information or data relation to data) or carrying out any operation or set of operations on the information or data, including:

a) organisation, adaptation or alteration of the information or data;
b) retrieval, consultation orthe use of the information or data;
c) disclosure of the information or data by transmission, dissemination or otherwise

making available; or
d) alignment, combination, blocking erasure or destruction of the information or data. [DPA 1998]

Relevant filing system: any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible. [DPA 1998]

Sensitive Personal Data: personal data consisting of information as to:

a) the racial or ethnic origin of the data subject
b) his political opinions
c) his religious beliefs or other beliefs of a similar nature
d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidations) Act 1992)
e) his physical or mental health or condition
f) his sexual life
g) the commission or alleged commission by him of any offence
h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings. [DPA 1998]

Third Party: any person other than:

a) the data subject;
b) the data controller; or
c) any data processor or other person authorised to process data for the data controller or processor. [DPA 1998]

Appendix 2: Polaris Medical Services Limited Application for Access to Personal Records for a Deceased Person

Application Reference Number: …… (office use only)

Please complete the following details in full: (please use an additional sheet if there is insufficient room)

Data Subject's details

Surname: ……

Maiden Name: ……(Or any previous surnames)
Forename(s): ……...

Address: ……...

……

…….. Post code: ……..…

Previous Address (if less than 3 years at above address)

……

……

…….. Post code: ……..…

Date of Birth: ……

Description of Information Required.....……...

……

Any additional details (such as relevant dates, contact names, references, where treated etc.)

……

……

Dates to be searched. From:.....……To……

Please complete this section with your details:

Surname: ……Forename(s): ……

Address: ……..

…….. Post code: ……
Relationship to data subject: ……

DECLARATION

I declare that the information given by me is, to the best of my knowledge, correct, and that I am entitled to apply for access to the information referred to above, under the terms of the

Access to Health Records Act 1990. (Please note that someone who knows you must witness your signature and must sign and complete the witness statement below.)

Signature of Applicant……Date: ……

Please confirm in what capacity you have signed by deleting the non-applicable alternatives:

- I am the deceased patient's personal representative and attach confirmation of my appointment*
- I have a claim arising from the patient's death on the grounds that*

……

……

……

……

WITNESS STATEMENT

I certify that I, (Name): ..…… of (Address): ...……

……Postcode: ……

have known the applicant named above for ……years as an employee/client/patient/personal friend* and have witnessed the applicant sign this form.

Signed: …… Date: ……

*Please delete as appropriate.

Please note as you are making an application on the behalf of somebody else we require evidence of your authority to do so i.e. personal authority, court order etc.

Please return this form together with proof of identity to:

The Information Governance Manager

Polaris Medical Services Limited

Mountbatten House

Dedworth road

Windsor

Berks

SL4 4LL

Appendix 3: Application for Data Subject Access Request

Application Reference Number: …… (office use only)

Please complete the following details in full for the data subject:

Surname: …… Forename(s): ……...
Maiden Name: …….. (Or any previous surnames)
Address: ……..……...

…… Post code: ...……
Previous Address (if less than 3 years at above address) ……..

…… Post code: ...……

Date of Birth: ……

Description of Information Required.....…….....

……

……
Additional details (such as relevant dates, contact names, references, where treated etc.)

……..

……
Dates to be searched: From: ..... To:…….……

Please complete this section if you are applying on behalf of the data subject

Surname: …… Forename(s):……...
Address: ……..

…… Post code: ...……
Relationship to data subject: ……

DECLARATION

I declare that the information given by me is, to the best of my knowledge, correct, and that I am entitled to apply for access to the information referred to above, under the terms of the Data Protection Act 1998. (Please note that someone who knows you must witness your signature and must sign and complete the witness statement below.)

Signature of Applicant……

Please confirm in what capacity you have signed by deleting the non-applicable alternatives.

- I am the data subject*
- I have been asked to act by the data subject and attach the data subject's written authorisation*
- I am the legal parent*/guardian* of the data subject who is under the age of 16 and who:
    - Is incapable of understanding the request*
    - Has consented to my making this request and their written authorisation is attached*
- I am the deceased data subject's personal representative and attach confirmation of my appointment*

- I have a claim arising from the data subject's death on the grounds that*

……

……

WITNESS STATEMENT

I certify that I, (Name): ..…… of Address:

...……...…

…… Post code: ...……

have known the applicant named above for ……years as an employee/ client/ patient/ personal friend* and have witnessed the applicant sign this form.

Signed: …… Date: ……

*Please delete as appropriate.

Please note: if you are making an application on the behalf of somebody else we require evidence of your authority to do so i.e. personal authority, court order etc.

Please return this form, marking the envelope 'Confidential', together with proof of identity (see below) and the relevant fee to:

The Information Governance Manager

Polaris Medical Services Limited

Mountbatten House

Dedworth Road

Windsor

Berks

SL4 4LL

A fee of £10 is payable per application under the Data Protection Act 1998. This fee may be increased to a maximum of £50 to cover the costs to the company for preparing non-computer held records. **Please make cheques payable to 'Polaris Medical Services Limited'**.

Suitable proofs of identity are: Passport, birth certificate, utility bills showing name and address.