**St Heliers Medical Practice**

**General Data Protection Regulation (GDPR) Policy**

**(incorporating Caldicott and Confidentiality)**

## Policy statement

The EU General Data Protection Regulation (GDPR herein) came into force on 25 May 2018; the Data Protection Act 2018 (DPA 2018) is to be read in conjunction with the GDPR. The GDPR applies to all EU member states and St Heliers Medical Practice must be able to demonstrate compliance at all times. Understanding the requirements of the GDPR will ensure that personal data of both staff and patients is protected accordingly.

## Status

This document and any procedures contained within it are contractual and therefore form part of your contract of employment. Employees will be consulted on any modifications or change to the document’s status.

## Training and support

The Practice will provide guidance and support to help those to whom it applies understand their rights and responsibilities under this policy. Additional support will be provided to managers and supervisors to enable them to deal more effectively with matters arising from this policy.

# Scope

## Who it applies to

This document applies to all employees, partners and directors of the practice. Other individuals performing functions in relation to the Practice, such as agency workers, locums and contractors, are encouraged to use it.

## Why and how it applies to them

All personnel at St Heliers Medical Practice have a responsibility to protect the information they process. This document has been produced to enable all staff to understand their individual and collective responsibilities in relation to the GDPR.

The Practice aims to design and implement policies and procedures that meet the diverse needs of our service and workforce, ensuring that none are placed at a disadvantage over others, in accordance with the Equality Act 2010. Consideration has been given to the impact this policy might have in regard to the individual protected characteristics of those to whom it applies.

# Definition of terms

## Data Protection Act 2018

The Data Protection Act 2018 (DPA 2018) is a complete data protection system, covering general data, law enforcement data and national security data.

## Data Protection Officer

An expert on data privacy, working independently to ensure compliance with policies and procedure.

## Data Protection Authority

National authorities tasked with the protection of data and privacy.

## Data Controller

The entity that determines the purposes, conditions and means of the processing of personal data.

## Data Processor

The entity that processes data on behalf of the Data Controller.

## Data Subject

A natural person whose personal data is processed by a controller or processor.

## Personal data

Any information related to a natural person or ‘data subject’.

## Processing

Any operation performed on personal data, whether automated or not.

## Recipient

The entity to which personal data is disclosed.

# The build-up to the GDPR

## Background

The GDPR is based on the 1980 Protection of Privacy and Transborder Flows of Personal Data Guidelines, which outlined eight principles:

* Collection limitation
* Data quality
* Purpose specification
* Use limitation
* Security safeguards
* Openness
* Individual participation
* Accountability

## NHS Digital

The Information Governance Alliance (IGA) is the authority that gives advice and guidance on the rules governing the use and sharing of healthcare-related information for the NHS. NHS Digital provides up-to-date information regarding the GDPR as well as a range of useful guidance documentation.[[1]](#footnote-1)

## Aim of the GDPR

The GDPR was designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens’ data privacy and to reshape the way in which organisations across the region approach data privacy.[[2]](#footnote-2)

## Brexit and the GDPR

Despite leaving the EU, the GDPR will still be enforced as it applies prior to the UK leaving the EU. The Regulation became applicable as law in the UK as of the 25th May 2018.

**GDPR and DPA18**

To ensure that organisations have a complete overview of the legislation, it will be necessary to view the GDPR and DPA 2018 side by side.[[3]](#footnote-3)

# Roles of data controllers and processors

## Data controller

At St Heliers Medical Practice the role of the data controller is to ensure that data is processed in accordance with Article 5 of the Regulation. He/she should be able to demonstrate compliance and is responsible for making sure data is:[[4]](#footnote-4)

* Processed lawfully, fairly and in a transparent manner in relation to the data subject
* Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
* Adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed
* Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay
* Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed
* Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

The data controller at St Heliers Practice is Karen Richards, Executive Manager; they are responsible for ensuring that all data processors comply with this policy and the GDPR.

## Data processor

Data processors are responsible for the processing of personal data on behalf of the data controller. Processors must ensure that processing is lawful and that at least one of the following applies:[[5]](#footnote-5)

* The data subject has given consent to the processing of his/her personal data for one or more specific purposes
* Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract
* Processing is necessary for compliance with a legal obligation to which the controller is subject
* Processing is necessary in order to protect the vital interests of the data subject or another natural person
* Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
* Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

At St Heliers Medical Practice, all staff are classed as data processors as their individual roles will require them to access and process personal data.

## 4 Data subject’s rights

All data subjects have a right to access their data and any supplementary information held by St Heliers Medical Practice. Data subjects have a right to receive:

* Confirmation that their data is being processed
* Access to their personal data
* Access to any other supplementary information held about them

St Heliers Medical Practice ensures that all patients are aware of their right to access their data and has privacy notices displayed in the following locations:

* Waiting room
* Practice website
* Practice information leaflet

To comply with the GDPR, all practice privacy notices are written in a language that is understandable to all patients and meet the criteria detailed in Articles 12, 13 and 14 of the GDPR.

The reason for granting access to data subjects is to enable them to verify the lawfulness of the processing of data held about them. In addition, data subjects can authorise third-party access, e.g. for solicitors and insurers, under the GDPR.

## Fees

Under the GDPR, St Heliers Medical Practice is not permitted to charge data subjects for initial access; this must be done free of charge. 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 practice to charge for all subsequent access requests.[[6]](#footnote-6)

The fee is to be based on the administrative costs associated with providing the requested information.

## Responding to a data subject access request

In accordance with the GDPR, data controllers must respond to all data subject access requests within one month of receiving the request (previous subject access requests had a response time of 40 days). It is the guidance of the BMA that a universal approach is applied and a 28-day response time implemented.6

In the case of complex or multiple requests, the data controller may extend the response time by a period of two months. In such instances, the data subject must be informed and the reasons for the delay explained.

## Verifying the subject access request

It is the responsibility of the data controller to verify all requests from data subjects using reasonable measures. The use of the practice Subject Access Request (SAR) form supports the data controller in verifying the request. In addition, the data controller is permitted to ask for evidence to identify the data subject, usually by using photographic identification, i.e. driving licence or passport.

## E-requests

The GDPR states that data subjects should be able to make access requests via email. St Heliers Medical Practice is compliant with this and data subjects can complete an e-access form and submit the form via email.

The data controller is to ensure that ID verification is requested and this should be stated in the response to the data subject upon receipt of the access request. It is the responsibility of the data controller to ensure they are satisfied that the person requesting the information is the data subject to whom the data applies.

## Third-party requests

Third-party requests will continue to be received following the introduction of the GDPR. The data controller must be able to satisfy themselves that the person requesting the data has the authority of the data subject.

The responsibility for providing the required authority rests with the third party and is usually in the form of a written statement or consent form, signed by the data subject.

St Heliers Medical Practice will request that third parties complete an appropriate request form.

## Requests from insurers

The Information Commissioner’s Office (ICO) refers to the use of SARs to obtain medical information for insurance purposes as being in fact an abuse of access rights, and the processing of full medical records by insurance companies risks breaching the GDPR.

Therefore, St Heliers Medical Practice will contact the patient to explain the extent of disclosure sought by the third party. The practice can then provide the patient with the medical record as opposed to the insurer. The patient is then given the opportunity to review their record and decide whether they are content to share the information with the insurance company.

St Heliers Medical Practice will advise insurers to use the Access to Medical Reports Act 1988 when requesting a GP report. Appropriate fees will be applicable.

**Solicitor Request**

A patient can authorise their solicitor or another third party to make a SAR. As long as the solicitor has provided the patient’s written consent to authorise access to the records, the SAR process should be followed as usual.

**Police Requests**

The Police may, on occasion, request access to personal data of individuals. Whilst there is an exemption in the Data Protection Act which permits the Practice to disclose information to support the prevention and detection of crime, the Police have no automatic right to access; however they can obtain a Court Order.

The Practice is a Data Controller and can only provide information held by the organisation. Data controllers in their own right must be applied to directly, the Practice will not transfer requests from one organisation to another.

**Application**

Individuals wishing to exercise their right of access should:

* Make a written application to the Practice holding the records, including via email
* Provide such further information as the Practice may require to sufficiently identify the individual (by completing the practice Data Request and Consent form)
* The Practice as “data controller” is responsible for ascertaining the purpose of the request and the manner in which the information is supplied.

**The Release Stage**

The format of the released information must comply with the requester’s wishes. Where no specific format is requested, the Practice should provide the information in the same manner as the original request. For example, requests received via email can be satisfied via email.

The release of a health record is subject to consultation with either:

* The health professional who is currently, or was most recently, responsible for the clinical care of the data subject in connection with the information which is the subject of the request
* Where there is more than one such health professional, the health professional who is the most suitable to advise on the information which is the subject of the request

Once the records have been collated, redacted where applicable and signed off by the Caldicott Lead, they should be sent to the requester. On no account must the original record be released. In denying or restricting access, a reason for the decision does not need to be given but the applicant should be directed through the appropriate complaint channels. Where information is not readily intelligible, an explanation (e.g. of abbreviations or terminology) must be given. If it is agreed that the subject or their representative may directly inspect the record, a health professional or HR administrator must supervise the access. If supervised by an administrator, this person must not comment or advise on the content of the record and if the applicant raises enquiries, an appointment with a health professional must be offered

**Exemptions**

Access may be denied or restricted where:

* The record contains information which relates to or identifies a third party that is not a care professional and has not consented to the disclosure. If possible, the individual should be provided with access to that part of the record which does not contain the third party information
* Access to all or part of the record will prejudice the carrying out of social work by reason of the fact that serious harm to the physical or mental well-being of the individual or any other person is likely. If possible the individual should be provided with access to that part of the record that does not post the risk of serious harm
* Access to all or part of the record will seriously harm the physical or mental well-being of the individual or any other person. If possible the individual should be provided with access to that part of the record that does not pose the risk of serious harm
* If an assessment identifies that to comply with a SAR would involve disproportionate effort under section 8(2)(a) of the Data Protection Act

There is no requirement to disclose to the applicant the fact that certain information may have been withheld.

In addition, Article 23 of the GDPR enables Members States, such as the United Kingdom to introduce further exemptions from the GDPR’s transparency obligations and individual rights. The Data Protection Officer can provide further information regarding exemptions applicable at the time of receipt of the subject access request.

**Complaints and Appeals**

The applicant has the right to appeal against the decision of the Practice to refuse access to their information. This appeal should be made to Karen Richards, Executive Manager/DPO.

If an applicant is unhappy with the outcome of their access request, the following complaints channels should be offered:

* meet with the applicant to resolve the complaint locally
* Advise a patient to make a complaint through the complaint’s process
* Advise a member of staff to consult with their trade union representative

If individuals remain unhappy with the Practice response, they have the right to appeal to the Information Commissioner’s Office:

<https://www.ico.org.uk/Global/contact_us>.

Information Commissioner’s Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Telephone: 0303 123 1113 Email: [casework@ico.gsi.gov.uk](mailto:casework@ico.gsi.gov.uk)

**Roles and Responsibilities**

The Caldicott Lead has executive responsibility for Subject Access Requests.

The Data Protection Officer has operational responsibility for Subject Access Requests.

All staff must be aware of how to recognise and manage a subject access request. Training will be provided to staff likely to be in receipt of requests covering:-

* Required format of a subject access request
* Correct identification of the requesting individual
* Location of personal information
* Timescales for compliance
* Provision of information in an intelligible format
* Action to be taken if the information includes third party data or if it has been determined that access will seriously harm an individual (see exemptions)

**Monitoring and Review of SARS**

Sara Burden/ Secretary, monitors all Subject Access Requests to ensure the correct process has been followed and escalates any appeals/complaints relating to Subject Access Requests to the practice DPO.

**Equality Impact**

In applying this policy, the organisation will have due regard for the need to eliminate unlawful discrimination**,** promote equality of opportunity**,** and provide for good relations between people of diverse groups, in particular on the grounds of the following characteristics protected by the Equality Act (2010); age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, and sexual orientation, in addition to offending background, trade union membership, or any other personal characteristic

# Data breaches

## Data breach definition

A data breach is defined as any incident that has affected the confidentiality, integrity or availability of personal data.[[7]](#footnote-7) Examples of data breaches include:

* Unauthorised third-party access to data
* Loss of personal data
* Amending personal data without data subject authorisation
* The loss or theft of IT equipment which contains personal data
* Personal data being sent to the incorrect recipient

## Reporting a data breach

Any breach that is likely to have an adverse effect on an individual’s rights or freedoms must be reported. In order to determine the requirement to inform the ICO, to notify them of a breach, the data controller is to read this supporting [guidance](https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf).

Breaches must be reported without undue delay or within 72 hours of the breach being identified.

When a breach is identified and it is necessary to report the breach, the report is to contain the following information:

* Organisation details
* Details of the data protection breach
* What personal data has been placed at risk
* Actions taken to contain the breach and recover the data
* What training and guidance has been provided
* Any previous contact with the Information Commissioner’s Office (ICO)
* Miscellaneous support information

The ICO data protection breach notification [form](https://ico.org.uk/media/for-organisations/documents/2666/security_breach_notification_form.doc) should be used to report a breach. Failure to report a breach can result in a fine of up to €10 million.[[8]](#footnote-8)

The DPO is to ensure that all breaches at St Heliers Medical Practice are recorded; this includes:

* Documenting the circumstances surrounding the breach
* The cause of the breach; was it human or a system error?
* Identifying how future incidences can be prevented, such as training sessions or process improvements

## Notifying a data subject of a breach

The data controller must notify a data subject of a breach that has affected their personal data without undue delay. If the breach is high risk (i.e. a breach that is likely to have an adverse effect on an individual’s rights or freedoms), then the data controller is to notify the individual before they notify the ICO.

The primary reason for notifying a data subject of a breach is to afford them the opportunity to take the necessary steps in order to protect themselves from the effects of a breach.

When the decision has been made to notify a data subject of a breach, the data controller at St Heliers Medical Practice is to provide the data subject with the following information in a clear, comprehensible manner:

* The circumstances surrounding the breach
* The details of the person who will be managing the breach
* Any actions taken to contain and manage the breach
* Any other pertinent information to support the data subject

St Heliers maintains a data breach log.

# Data erasure

## Erasure

Data erasure is also known as the “right to be forgotten”, which enables a data subject to request the deletion of personal data where there is no compelling reason to retain or continue to process this. information. It should be noted that the right to be forgotten does not provide an absolute right to be forgotten; a data subject has a right to have data erased in certain situations.

The following are examples of specific circumstances for data erasure:

* Where the data is no longer needed for the original purpose for which it was collected
* In instances where the data subject withdraws consent
* If data subjects object to the information being processed and there is no legitimate need to continue processing it
* In cases of unlawful processing
* The need to erase data to comply with legal requirements

The data controller can refuse to comply with a request for erasure in order to:

* Exercise the right for freedom of information or freedom of expression
* For public health purposes in the interest of the wider public
* To comply with legal obligations or in the defence of legal claims

## Notifying third parties about data erasure requests

Where St Heliers Medical Practice has shared information with a third party, there is an obligation to inform the third party about the data subject’s request to erase their data; this is so long as it is achievable and reasonably practical to do so.

This policy will be updated once the NHS IGA have issued guidance regarding data erasure.

# Consent

## Appropriateness

Consent is appropriate if data processors are in a position to “offer people real choice and control over how their data is used”.[[9]](#footnote-9) The GDPR states that consent must be unambiguous and requires a positive action to “opt in”, and it must be freely given. Data subjects have the right to withdraw consent at any time.

## Obtaining consent

If it is deemed appropriate to obtain consent, the following must be explained to the data subject:

* Why the practice wants the data
* How the data will be used by the practice
* The names of any third-party controllers with whom the data will be shared
* Their right to withdraw consent at any time

All requests for consent are to be recorded, with the record showing:

* The details of the data subject consenting
* When they consented
* How they consented
* What information the data subject was told

Consent is to be clearly identifiable and separate from other comments entered into the healthcare record. At St Heliers Medical Practice it is the responsibility of the data controller Karen Richards, Executive Manager to demonstrate that consent has been obtained. Furthermore, the data controller must ensure that data subjects (patients) are fully aware of their right to withdraw consent, and must facilitate withdrawal as and when it is requested.

# Data mapping and Data Protection Impact Assessments

## Data mapping

Data mapping is a means of determining the information flow throughout an organisation. Understanding the why, who, what, when and where of the information pathway will enable St Heliers Medical Practice to undertake a thorough assessment of the risks associated with current data processes.

Effective data mapping will identify what data is being processed, the format of the data, how it is being transferred, if the data is being shared, and where it is stored.

St Heliers completed a data mapping exercise in August 2018.

An action plan was agreed as a result.

## Data mapping and the Data Protection Impact Assessment

Data mapping is linked to the Data Protection Impact Assessment (DPIA), and when the risk analysis element of the DPIA process is undertaken, the information ascertained during the mapping process can be used.

Data mapping is not a one-person task; all staff at St Heliers Medical Practice will be involved in the mapping process, thus enabling the wider gathering of accurate information.

## Data Protection Impact Assessment

The DPIA is the most efficient way for St Heliers Medical Practice to meet its data protection obligations and the expectations of its data subjects. DPIAs are also commonly referred to as Privacy Impact Assessments or PIAs.

In accordance with [Article 35](https://gdpr-info.eu/art-35-gdpr/) of the GDPR, DPIA should be undertaken where:

* A type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons; then the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
* Extensive processing activities are undertaken, including large-scale processing of personal and/or special data

DPIAs are to include the following:

* A description of the process, including the purpose
* An evaluation of the need for the processing in relation to the purpose
* An assessment of the associated risks to the data subjects
* Existing measures to mitigate and control the risk(s)
* Evidence of compliance in relation to risk control

It is considered best practice to undertake DPIAs for existing processing procedures to ensure that St Heliers Medical Practice meets its data protection obligations. DPIAs are classed as “live documents” and processes should be reviewed continually. As a minimum, a DPIA should be reviewed every three years or whenever there is a change in a process that involves personal data.

## DPIA process

The DPIA process is formed of the following key stages:

* Determining the need
* Assessing the risks associated with the process
* Identifying potential risks and feasible options to reduce the risk(s)
* Recording the DPIA
* Maintaining compliance and undertaking regular reviews

# Caldicott

This section applies to all patient-identifiable information processed, stored on computer or relevant filing systems (manual records) and the Practice staff who use the information in connection with their work.

The Practice will take all necessary steps to safeguard the integrity, confidentiality, and availability of sensitive information.

No staff member employed by the Practice (including temporary or agency staff) is allowed to share any patient-identifiable information unless it has been authorised by the Practice’s Caldicott

Guardian.

**Caldicott Guarian Role**

St Heliers Medical Practice has appointed Dr A Ali as its Caldicott Guardian.

The Guardian is responsible for the establishment of procedures governing access to, and the use of patient-identifiable information and, where appropriate, the transfer of that information to other bodies.

In addition to the principles developed in the Caldicott Report, the Guardian must also take account of the codes of conduct provided by professional bodies, and guidance on the Protection and Use of Patient Information and on IM&T security disseminated by the Department of Health.

They must also, where necessary, provide advice and support to staff working within the Practice on all aspects of Caldicott, sharing and disclosure of patient-identifiable patient information and related legislation.

It is unlikely that any authorisation to share patient-identifiable data will be granted unless the access is on a need to know basis and justifiable against the Caldicott principles.

The Caldicott standard is based on the following six principles:

* 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.
* Don’t use patient-identifiable information unless it is absolutely necessary - Patient-identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
* Use the minimum necessary patient-identifiable information - Where use of patient-identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.
* 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. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.
* Everyone with access to patient-identifiable information 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 made fully aware of their responsibilities and obligations to respect patient confidentiality.
* Understand and comply with the law – Every use of patient-identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.

**Confidentiality**

**The Practice’s Responsibilities**

The practice will ensure that employees fully understand all their responsibilities with regard to confidential data, by ensuring employees undertake Information Governance training and sign a written statement of the responsibilities they are undertaking towards the security of all data within the surgery. Competency will be assessed as an ongoing process and as part of the appraisal process.

The practice will complete and submit the DSP Toolkit self-assessment on an annual basis.

The practice will also ensure that arrangements are in place for the confidential disposal of any paper waste generated at work. Care should be taken to ensure that the company are accredited to destroy sensitive papers. Records should be kept of the registration of the company and a log of collections.

The practice strictly applies the rules of confidentiality and will not release patient information to a third party (other than those involved in the direct care of a patient) without proper valid and informed consent, unless this is within the statutory exempted categories such as in the public interest, or if required by law, in which case the release of the information and the reasons for it will be individually and specifically documented and authorised by the responsible clinician.

All staff at St Heliers Medical Practice are to adhere to the principles of confidentiality outlined in the

[NHS(E) Confidentiality Policy](https://www.england.nhs.uk/wp-content/uploads/2016/12/confidentiality-policy-v3-1.pdf).

**Good practice**

The following actions at St Heliers Medical Practice will be undertaken to ensure that confidentiality is maintained:

* Person-identifiable information will be anonymised so far as is reasonably practicable, whilst being mindful of not compromising the data
* Access to consulting rooms, administrative areas and record-storage areas will be restricted
* A clear-desk policy is in operation at all times, and is applicable to all staff
* All IT equipment is shut down at the end of the working day
* Smart Cards are to be removed from the computer whenever the user leaves their workstation
* Confidential waste is shredded or disposed of appropriately

Furthermore, staff will not:

* Talk about patients or confidential information in areas where they may be overheard
* Leave computers or other equipment logged on
* Leave Smart Cards unattended or share their cards with other staff members
* Leave any patient confidential information in unsecured areas at any time
* The supplier of our clinical software manages the anti-virus software version control and ensures it is regularly updated.
* New programmes should not be downloaded without the permission of the IT or practice manager. This reduces the risk of malware being downloaded and affecting the computer.

**Confidentiality Breach**

Any breach of confidentiality must be recorded in the practice incident book and reported immediately to Karen Richards, Executive Manager (Irene Bagnall Service Manager in her absence). All breaches will be recorded

# Summary

Given the complexity of the GDPR, all staff at St Heliers Medical Practice must ensure that they fully understand the requirements within the Regulation. Understanding the Regulation will ensure that personal data at St Heliers Medical Practice remains protected and the processes associated with this data are effective and correct.

Regular updates to this policy will be applied when further information and/or direction is received.

**Appendix A: Form – Subject Access Request Form**

|  |  |
| --- | --- |
| St Heliers Medical Practice respects the rights of individuals to have copies of their information wherever possible. | |
| **Personal information collected from you by this form, is required to enable your request to be processed, this personal information will only be used in connection with the processing of this Subject Access Request.** | **DPA_Padlock__blue_** |
| **Charges Payable:** In accordance with legislation **no fee** will be charged for your request, unless the request is manifestly unfounded or excessive, particularly if it is repetitive. Before any further action is taken, we will contact you with details of our “reasonable administrative charges” in order to comply with your request. | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **PLEASE COMPLETE IN BLOCK CAPITALS – Illegible forms will delay the time taken to respond to requests.** | | | | | | | | | | | | | | | | | |
| **1.** | | **Details of Patient/Clients/Staff members records to be accessed** (Please complete one form per person) | | | | | | | | | | | | | | | |
| Surname | | | | | | | | | | | | | | Date of Birth | | | |
| Forename(s) | | | | | | | | | | | | | | Current Address  Full Postcode | | | |
| Any former names (If Applicable) | | | | | | | | | | | | | |
| Telephone Number | | | | | | | | | | | | | | Previous Address (If Applicable)  Full Postcode | | | |
| NHS Number (If known/relevant) | | | | | | | | | | | | | |
|  |  | |  | |  |  |  | |  |  | |  |  |
| If further details are available please include in a separate covering note. | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | |
| **2.** | | **Details of Records to be Accessed** | | | | | | | | | | | | | | | |
| In order to locate the records you require please provide as much information as possible. Please list the department or services you have accessed that you require records from: i.e. PALs, complaints, continuing healthcare or Human resources etc (Continue on a separate sheet if required). | | | | | | | | | | | | | | | | | |
| **Records dated from** | | | | | | | | **Department or services accessed** | | | | | | | | | |
| / / **to** / / | | | | | | | |  | | | | | | | | | |
| / / **to** / / | | | | | | | |  | | | | | | | | | |
| / / **to** / / | | | | | | | |  | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | |
| **3.** | | **Details of applicant** (Complete if different to patients/clients/staff members details) | | | | | | | | | | | | | | | |
| Full Name | | | | | | | |  | | | | | | | | | |
| Company (if Applicable) | | | | | | | |  | | | | | | | | | |
| Relationship with individual who’s records have been requested | | | | | | | | | | |  | | | | | | |
| Address to which a reply should be sent | | | | | | | | **Postcode: Tel:** | | | | | | | | | |
| **4.** | | **Authorisation to release to applicant** (to be completed by the patients/clients/staff memberif not making their own request) | | | | | | | | | | | | | | | |
| **I (Print name)** hereby authorise St Heliers Medical Practice to release any personal data they may hold relating to me to the above applicant and to whom I authorise to act on my behalf.  **Signature of** patient/client/staff member **:** **Date:** / / | | | | | | | | | | | | | | | | | |
| **5.** | | **Declaration** | | | | | | | | | | | | | | | |
| I declare that information given by me is correct to the best of my knowledge and that I am entitled to apply for access to the health record(s) referred to above, under the terms of the Access to Health Records Act (1990) / Data Protection Act.  **Please select one box below:**  ❑ I am the patient/client/staff member (data subject).  ❑ I have been asked to act on behalf of the data subject and they have completed section 4 -authorisation above.  ❑ I am acting on behalf of the data subject who is unable to complete the authorisation section above (Covering letter with further details supplied).  ❑ I am the parent/guardian of a data subject under 16 years old who has completed the authorisation section above. (Please include proof such as birth certificate)  ❑ I am the parent/guardian of a data subject under 16 years old who is unable to understand the request and who has consented to my making the request on their behalf.  ❑ I have been appointed the Guardian for the patient/client, who is over age 16 under a Guardianship order (attached).  ❑ I am the deceased patient/client’s personal representative and attach confirmation of my appointment.  ❑ I have a claim arising from the patient/client’s death and wish to access information relevant to my claim (Covering letter with further details to be supplied). | | | | | | | | | | | | | | | | | |
| **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. * It may be necessary to provide evidence of identity (i.e. Driving Licence). * If there is any doubt about the applicant’s identity or entitlement, information will not be released until further evidence is provided. You will be informed if this is the case. * Under the terms of the Data Protection Act, Subject Access Requests will be responded to within 30 days after receiving all necessary information and/or fee required to process the request. * If you are making a request under the Access to Health Records Act 1990, requests will be responded to within 40 days where no entries have been made to the patient/client’s record 40 days immediately preceding the date of this request, otherwise requests will be responded to within 21 days after receiving all necessary information and/or fee required to process the request. * Under the terms of Section 7 of the Data Protection Act, Information disclosed under a Subject Access Request may have information removed; this is to ensure that the confidentiality is maintained for third parties referred to who have not consented to their information being disclosed. | | | | | | | | | | | | | | | | | |
| **Print Name** | | | |  | | | | | | | **Signed (Applicant)** | | | |  | **Date** | / / |

**Please complete and send this document to: St Heliers Medical Practice, 15 St Heliers Road,  
Northfield, B31 1QT**

Do you reasonably require more information to process the request?

Do you hold information relating to the data subject?

**Appendix B: Subject Access Request Flow Diagram**

Has a subject access request been received in writing (completed SAR form or via email)?

NO

NO

YES

Notify the data subject in writing that the information is exempt from disclosure

Notify the data subject in writing that the information cannot be disclosed

Has all the information to be released been reviewed by the clinical lead / IAO and redacted before submission to the Caldicott Lead?

Can the information be provided without including references to a third party (even after redaction)?

YES

NO

Clinical lead / IAO to conduct review and redaction process

APPROVED

Release information

Package information and covering letter for approval by the Caldicott Lead

YES

Notify the data subject in writing that no information is held by the PRACTICE

YES – acknowledge receipt of the request, log and assign a reference number

NO

YES

NO

Advise requester that the request must be in writing (either using the SAR Form or via email)

Do any exemptions from disclosure apply?

Request additional supporting information from requester and advise that the one calendar month response timeframe will only apply once all outstanding information has been received.

1. [NHS Digital GDPR guidance](https://www.digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance) [↑](#footnote-ref-1)
2. [EU GDPR overview](https://www.eugdpr.org/eugdpr.org.html) [↑](#footnote-ref-2)
3. [IGA The General Data Protection Regulation What’s New](https://digital.nhs.uk/media/35499/IGA-GDPR-What-s-new-guidance-V1-FINAL/pdf/IGA_-_GDPR_What's_new_guidance_V1_FINAL) [↑](#footnote-ref-3)
4. [Article 5 GDPR Principles relating to processing of personal data](https://gdpr-info.eu/art-5-gdpr/) [↑](#footnote-ref-4)
5. [Article 6 Lawfulness of processing](https://gdpr-info.eu/art-6-gdpr/) [↑](#footnote-ref-5)
6. [BMA Guidance – Access to health records](https://www.bma.org.uk/-/media/files/pdfs/employment%20advice/ethics/access-to-health-records-may2018.pdf?la=en) [↑](#footnote-ref-6)
7. [ICO – Personal data breaches](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/) [↑](#footnote-ref-7)
8. [ICO Personal data breaches](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/) [↑](#footnote-ref-8)
9. [ICO Consent](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/) [↑](#footnote-ref-9)