Information Rights Protocol (barring SAR)

|  |  |  |
| --- | --- | --- |
| Policy Title / Reference | Author | Owner |
| Information Rights and Access Protocol | Emma Cooper, Cluster DPO (Kafico) | Practice Manager |

|  |  |  |
| --- | --- | --- |
| Version | Revision author | Version comments |
| 1 | Emma Cooper, Kafico Ltd, DPO | New Draft |
| 2 | Emma Cooper, Kafico Ltd - DPO | Removal of SAR elements to be put into a separate Protocol |
| 2.1 | Emma Cooper, Kafico Ltd - DPO | Jan 2019 Replaced 1998 DPA with 2018 Act. Replaced GDPR with “data protection legislation”. Removed Rules of Thumb at the bottom as it relates to SARs. |
| 2.1 | Emma Cooper, Kafico Ltd - DPO | Jan / Feb 20 – Annual review – no amendments |

Contents

[2. Scope 2](#_Toc6744974)

[3. Definitions 3](#_Toc6744975)

[4. Introduction 3](#_Toc6744976)

[5. Statutory Mandatory Framework 3](#_Toc6744977)

[6. Accountable Parties 4](#_Toc6744978)

[7. The Right to be Informed 4](#_Toc6744979)

[8. Right to Rectification 5](#_Toc6744980)

[9. Right to Erasure 6](#_Toc6744981)

[10. Right to Restriction 7](#_Toc6744982)

[11. Right to Portability 8](#_Toc6744983)

[12. Right to Object 9](#_Toc6744984)

[13. Rights around Automated Decision Making and Profiling 10](#_Toc6744985)

[14. Associated Protocols 11](#_Toc6744986)

[15. Audit Schedule 12](#_Toc6744987)

[16. Review 12](#_Toc6744988)

[Appendix A: Information Access and Rights Process Flow 13](#_Toc6744989)

[Appendix A: Template Responses for Information Rights Requests 14](#_Toc6744990)

[Request for Rectification / Erasure (unable to action) 14](#_Toc6744991)

[Request for Rectification / Erasure / Objection (able to action) 15](#_Toc6744992)

# Scope

This protocol has been drafted for use by customers of Kafico Ltd across Suffolk.

At the time of writing and unless alternative protocols have been adopted locally, the protocol applies to;

|  |  |  |
| --- | --- | --- |
| Barrack Lane | Stanton (west) | Mendlesham |
| Burlington Road | Mount Farm | Wickhambrook |
| Framlingham | Swan and Forest | Church Farm Surgery (Aldeburgh) |
| Botesdale Health Centre | Glemsford | Framfield |
| Little St John Street | Lakenheath | Saxmundham |
| Hawthorn Drive | Ixworth | Guildhall & Barrow |
| The Surgery, Leiston | Ivry Street | Peninsula |
| Victoria Surgery | Grove Medical Centre | Felixstowe Road Medical Practice |

# Definitions

Personal Confidential Information This term is intended to cover information captured by the Data Protection Act 2018 / GDPR (identifiable information about the living), information covered by the Common Law Duty of Confidence / Tort of Misuse of Private Information and finally, information covered by Article 8 European Convention for Human Rights.

# Introduction

Data protection law provides data subjects (the individual that information is about) with a wide array of rights that must be observed by organisations that process personal data.

# Statutory Mandatory Framework

The General Data Protection Regulations provide the following rights for individuals:

* The right to be informed.
* The right of access.
* The right to rectification.
* The right to erasure.
* The right to restrict processing.
* The right to data portability.
* The right to object.
* Rights in relation to automated decision making and profiling.

# Accountable Parties

See Information Governance Policy for key roles.

All staff, whether management or administrative, who create, receive and use data have responsibilities to observe the information rights of data subjects. Employees have a contractual and legal obligation to read and comply with all company policies and to attend mandatory training to support the appropriate management of information.

# The Right to be Informed

Any activity that involves processing personal information should involve consideration of how individuals might be made aware and have an opportunity to object

The information to be supplied must be;

* concise, transparent, intelligible and easily accessible;
* written in clear and plain language, particularly if addressed to a child; and
* free of charge

These Privacy Notices should be multi-layered (i.e. website, leaflets, videos etc) and their placement should consider the target audience including variance in levels of age and comprehension.

|  |  |  |
| --- | --- | --- |
| **What information must be supplied?** | **Data obtained directly from data subject** | **Data obtained from a third party or sharing partner** |
| Identity and contact details of the controller (and where applicable, the controller’s representative) and the data protection officer |  |  |
| Purpose of the processing and the lawful basis for the processing |  |  |
| The legitimate interests of the controller or third party, where applicable |  |  |
| Categories of personal data |  |  |
| Any recipient or categories of recipients of the personal data |  |  |
| Details of transfers to third country and safeguards |  |  |
| Retention period or criteria used to determine the retention period |  |  |
| The existence of each of data subject’s rights |  |  |
| The right to withdraw consent at any time, where relevant |  |  |
| The right to lodge a complaint with a supervisory authority |  |  |
| The source the personal data originates from and whether it came from publicly accessible sources |  |  |
| Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data |  |  |
| The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences. |  |  |

# Right to Rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

If the information has been disclosed to third parties, they must be informed of the rectification where possible. Individuals must also be informed about the third parties to whom the data has been disclosed where appropriate.

Requests must be responded to within one month. This can be extended by two months where the request for rectification is complex.

There may be occasions, where there is a legal requirement to maintain the original data or where the accuracy of the data is contested – this should be raised with the Data Protection Officer to ensure appropriate management

Where not taking action in response to a request for rectification, the individual must be provided with an explanation, informing them of their right to complain to the Information Commissioner’s Office (ICO) and to a judicial remedy.

Where an individual contests the accuracy of the personal data, the processing should be restricted until the accuracy has been verified (see Section 9)

# Right to Erasure

The right to erasure is also known as ‘the right to be forgotten’. This right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

The right to erasure does not provide an absolute ‘right to be forgotten’. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

* Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
* When the individual withdraws consent.
* When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
* The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
* The personal data has to be erased in order to comply with a legal obligation.
* The personal data is processed in relation to the offer of information society services to a child.

If the processing does cause damage or distress, this is likely to make the case for erasure stronger.

There are some specific circumstances where the right to erasure **does not apply** and you can refuse to deal with a request;

* to exercise the right of freedom of expression and information;
* to comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
* for public health purposes in the public interest;
* archiving purposes in the public interest, scientific research historical research or statistical
* purposes; or the exercise or defence of legal claims.

Where a child has given consent to processing and they later request erasure of the data (regardless of age at the time of the request), consideration should be made as to how well they were originally made aware of the risks involved in processing in the first place.

If the personal information has been disclosed to third parties, they must be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

# Right to Restriction

Individuals have a right to request that their personal information is restricted.

When processing is restricted, **The Practice** are permitted to store the personal data, but not further process it. Just enough information may be retained about the individual to ensure that the restriction is respected in future.

Circumstances where the processing must be restricted are;

* Where an individual contests the accuracy of the personal data, the processing should be restricted until the accuracy has been verified
* Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and there is a need to consider whether your organisation’s legitimate grounds override those of the individual
* When processing is unlawful and the individual opposes erasure and requests restriction instead
* If the information is no longer needed but the individual requires the data to establish, exercise or defend a legal claim

If the personal data in question has been disclosed to third parties, they must be informed about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

When you decide to lift a restriction on processing, the individual must be informed.

# Right to Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The data must be provided in a structured, commonly used and machine-readable form.

Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.

The information must be provided free of charge, without delay and within one month.

If the individual requests it, you may be required to transmit the data directly to another organisation if this is technically feasible. However, it is not necessary for [insert practice name] to adopt or maintain processing systems that are technically compatible with other organisations.

Where the personal data concerns more than one individual, there must be consideration of whether providing the information would prejudice the rights of any other individual.

The right to data portability only applies:

* to personal data an individual has been provided to a controller by the individual;
* where the processing is based on the individual’s consent or for the performance of a
* contract; and
* when processing is carried out by automated means

# Right to Object

Individuals have the right to object to:

* processing based on legitimate interests or the performance of a task in the public
* interest/exercise of official authority (including profiling);
* direct marketing (including profiling); and
* processing for purposes of scientific/historical research and statistics

**Objections to processing personal data for the performance of a legal task or The Practice’s legitimate interests;**

Individuals must have an objection on “grounds relating to his or her particular situation”.

Processing of the personal data must be stopped unless:

* Compelling legitimate grounds can be demonstrated for the processing, which override the interests, rights and freedoms of the individual; or
* the processing is for the establishment, exercise or defence of legal claims.

Individuals must be explicitly informed of their right to object “at the point of first communication” and in the privacy notice and must be clear and separate from other information.

**Objections to processing personal data for direct marketing purposes**

Processing personal data for direct marketing purposes must be stopped as soon as an objection is received. There are no exemptions or grounds to refuse.

Objections to processing for direct marketing must be dealt with at any time and free of charge.

Individuals must be explicitly informed of their right to object “at the point of first communication” and in the privacy notice and must be clear and separate from other information.

**Objections to processing personal data for research purposes**

Individuals must have “grounds relating to his or her particular situation” in order to exercise their right to object to processing for research purposes.

If you are conducting research where the processing of personal data is necessary for the performance of a public interest task, you are not required to comply with an objection to the processing.

Where any of the above processing activities are carried out online, the individual must be offered a way to object online.

# Rights around Automated Decision Making and Profiling

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

Individuals have the right not to be subject to a decision when:

* it is based on automated processing; and
* it produces a legal effect or a similarly significant effect on the individual.

Individuals must be able to:

* obtain human intervention;
* express their point of view; and
* obtain an explanation of the decision and challenge it

The right **does not apply** if the decision:

* is necessary for entering into or performance of a contract between [insert practice name] and the individual;
* is authorised by law (e.g. for the purposes of fraud or tax evasion prevention); or
* based on explicit consent. (Article 9(2)).
* Furthermore, the right does not apply when a decision does not have a legal or similarly significant effect on someone

The GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular (where relevant to **The Practice**) to analyse or predict their:

* performance at work;
* health

When processing personal data for profiling purposes, appropriate safeguards must be in place;

* Ensure processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the envisaged consequences.
* Use appropriate mathematical or statistical procedures for the profiling.
* Implement appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
* Secure personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions taken for the purposes listed above must not:

* concern a child; or
* be based on the processing of special categories of data

**unless:**

* you have the explicit consent of the individual; or
* the processing is necessary for reasons of substantial public interest on the basis of UK law

This must be proportionate to the aim pursued, respect the essence of the right to data protection and provide suitable and specific measures to safeguard fundamental rights and the interests of the individual.

# Associated Protocols

This protocol should be read in conjunction with;

* Risk Management Policy
* Change Management Policy
* Information Governance Policy
* Information Rights and Access Protocol
* Information Sharing and Privacy Protocol
* Information Lifecycle and Data Quality Protocol
* Information / Cyber Security Protocol
* Information Incident Protocol
* Information Risk and Audit Protocol
* Data Protection Impact Assessment Protocol
* Freedom of Information Protocol

# Audit Schedule

Compliance with this protocol will be audited and the results fed into the Plan, Do, Check, Act Cycle described in the Information Risk and Audit Protocol.

# Review

This protocol will be reviewed every year or sooner where necessary.

# Appendix A: Information Access and Rights Process Flow

# Appendix A: Template Responses for Information Rights Requests

# Request for Rectification / Erasure (unable to action)

(Remember that the data subject has the right to request that their information is “restricted” which means it can no longer be accessed, shared or used in any way other than storage whilst the rest is being processed)

Dear [requestor],

We write in relation to the request you made on [insert date] to have your personal data removed from / amended within our system. The specifics of your request are detailed below for clarity.

1. [Please delete all the information you hold about my access to your services in 2017]

At [insert practice name], we make every effort to ensure that the information we hold about you is accurate and up to date we take your information rights very seriously.

Following your request, we [Identified the information concerned and discussed the source of the information and your request for amendment. We have liaised with your GP who has confirmed that the information is correctly recorded in your health record].

As a result, we have come to the conclusion that the information is accurate and therefore, we are unable to remove or amend this within your record.

We have a statutory requirement to ensure that our records are an accurate reflection of tasks carried out in the public interest and therefore cannot always respond to requests to amend records / delete records where we they are determined to be accurate / we are required to retain for statutory purposes..

We have, however, noted within your [insert practice name] record that this information is disputed by you.

You do have a right to make a complaint to us or the Information Commissioner, if you feel your request has not been managed appropriately. You can call them on 0303 123 1113 or write to them at;

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Additionally, you also have a right to seek to enforce your rights through the courts.

We understand that this is not the outcome you were seeking and we would be happy to discuss this with you further if required.

Sincerely,

[Caldicott Guardian}

# Request for Rectification / Erasure / Objection (able to action)

Dear [requestor],

We write in relation to the request you made in [insert date] to have your personal data removed from / amended within our system. The specifics of your request are detailed before for clarity.

1. [Please delete all the information you hold about my access to your services in 2017]

We have completed this erasure / rectification and can confirm that this information is no longer held within your record. At [insert practice name], we make every effort to ensure that we acknowledge and act on the information rights of patients appropriately.

We have a legal requirement to ensure that our records are an accurate reflection of events and disclosures. We have, therefore made the requested amendments to / removed the data from your records.

You do also have a right to make a complaint to the Information Commissioner, if you feel your request has not been managed appropriately. You can call them on 0303 123 1113 or write to them at;

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Additionally, you also have a right to seek to enforce your rights through the courts.

We would be happy to discuss this with you further if required.

Sincerely,

[Caldicott Guardian}