Stanton Surgery

Information Rights and Transparency Protocol

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Author | Next Review Date | Notes |
| V1 (March 22) | Emma Kitcher, DPO | March 23 | Should be read as new protocol that replaces IG04. Now includes Quick Reference Points, information about ‘no surprises’ – new Caldicott Principle. Added more comprehensive information about duty of confidentiality Added a number of case study examplesAdded the requirement to notify DPO when engaging clinical decision support tools under Section 11.Added Section 12 – Children and Young People. |
| V2 March 23 | Emma Kitcher, DPO | March 24 | Inserted Section 6 – Rights Management ProcessInserted Section 14 - Complaints |
| V2 (May 24)  | Emma Kitcher, DPO | January 2025 | The policies have been extended for the year to accommodate that new legislation is being enacted later in the year. |

**Contents**

[1. INTRODUCTION 2](#_Toc129365418)

[2. QUICK REFERENCE POINTS 2](#_Toc129365419)

[3. KEY DEFINITIONS 3](#_Toc129365420)

[4. SCOPE 3](#_Toc129365421)

[5. KEY LEGISLATION / FRAMEWORK 4](#_Toc129365422)

[ RIGHTS MANAGEMENT PROCESS 4](#_Toc129365423)

[6. RIGHT TO BE INFORMED / NO SURPRISES 4](#_Toc129365424)

[7. RIGHT TO RECTIFICATION 6](#_Toc129365425)

[8. RIGHT TO RESTRICTION 8](#_Toc129365426)

[9. RIGHT TO PORTABILITY 8](#_Toc129365427)

[10. RIGHT TO OBJECT 9](#_Toc129365428)

[11. AUTOMATED DECISION MAKING AND PROFILING 11](#_Toc129365429)

[12. CHILDREN AND YOUNG PEOPLE 13](#_Toc129365430)

[13. COMPLAINTS 14](#_Toc129365431)

[14. APPLICATION AND AUDIT 14](#_Toc129365432)

1. 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. Additionally, the human rights of service users, visitors and employees is underpinned by the notion of being informed, aware and being involved in decisions that affect them.

1. QUICK REFERENCE POINTS
* Patients, customers, service users, visitors and employees have;
	+ a right to be informed about how their personal data is used
	+ a right to access a copy of the personal data you hold about them
	+ a right to correct personal data when it is incorrect
	+ a right to have personal data erased
	+ a right to restrict you from accessing, sharing, transferring or altering their personal data
	+ a right to have their personal data sent (ported) to their new provider
	+ a right to object to you processing their personal data
	+ a right to know the details of automated decision making and profiling
	+ a right to autonomy and self determination
* When managing Personal Confidential Information, there should be ‘no surprises’ about how it is used
* These rights are not ‘absolute’ and there are times when they do not apply
1. KEY 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.

1. SCOPE

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 rights described in this protocol apply to customers, service users, visitors and employees.

1. KEY LEGISLATION / FRAMEWORK
* UK GDPR / Data Protection Act 2018
* Caldicott Principles
* Human Rights Act 1998
1. RIGHTS MANAGEMENT PROCESS

Where a patient, employee or visitor makes a request under data protection, staff should escalate to stanton.surgery@nhs.net who will review in accordance with the policy and engage the support of the Data Protection Officer. A log will be kept by the practice and / or the Data Protection Officer to ensure records of timely and lawful responses.

In the event of staff absence, the information rights lead at the practice will ensure that requests are handed over so that the DPO can continue to manage the request in their absence.

1. RIGHT TO BE INFORMED / NO SURPRISES
* Any activity that involves processing Personal Confidential 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.
* 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.

When considering activities that involve Personal Confidential Information consider;

* Is this something we already list in our privacy materials?
* Is this something that the average individual would expect me to do?
* Would a reasonable person be ‘highly offended’ if I did not contact them before I do this?

If the answer to any of the above questions is ‘no’, refer the activity to your Data Protection Officer who can assist with raising awareness.

* The concept of no surprises doesn’t mean that we ask for consent every time we undertake activity with Personal Confidential Information.

Example:

We are required to disclosure information about a person who poses a threat to the public. We believe that making them aware of the disclosure could trigger the threat we are trying to manage. We do not tell the individual or obtain consent. However, we already note in our privacy materials that we will make these kinds of disclosures. The average, reasonable person expects these types of disclosures and would not be ‘highly offended’ at the concept of protecting the public. Therefore, there are “no surprises”.

Example:

We are going to send someone for a blood test. To do this, we are going to send basic information about who they are and why they need a blood test to the hospital.

We do not make the patient sign a consent form to send their personal data to the hospital. This is because the average, reasonable person expects this type of disclosure and would not be ‘highly offended’ at the concept of their data being sent to the hospital for this purpose. Therefore, there are “no surprises”.

* Informing individuals about how their information is used supports their human rights.
* We all have a right to feel a sense of control over our lives. Involving individuals through transparency and engagement supports this control and autonomy.
1. 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.
* For example, if we work in a Multi-Disciplinary Team, we can share that the data was found to be inaccurate and advise the other team members to ensure their own records are altered.
* 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.

Example:

An employee claims that the minutes of a disciplinary meeting are incorrect and that they did not make the statements that are recorded about personal situations affecting their work. They insist that the record is amended. The parties present all attest to the accuracy of the record and so the individual is informed that the amendment will not be made since employment law requires them to maintain accurate notes of the formal disciplinary process. However, a note can be made on the record so that all recipients are aware that the employee contests the information in the minutes.

Example:

A patient claims that the notes of a consultation are incorrect and that whilst they had a mental health diagnosis in 2017, they now believe it to be an incorrect diagnosis and they want it removed from their record.

Having checked with the health professionals involved, the parties are in agreement that the diagnosis was made and that it is important it remains within their record.

The individual is informed that the amendment will not be made since there is a legal requirement to record events that occurred. However, a note can be made on the record so that all recipients are aware that the patient contests the information in the record and they are invited for a new assessment of their diagnosis.

* Where not taking action in response to a request for rectification, the individual must be provided with an explanation and the contact details of the Data Protection Officer, 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 Right to Restriction).
1. RIGHT TO RESTRICTION
* Individuals have a right to request that their personal data is restricted.
* When processing is restricted, you can still store the personal data, but cannot access, transmit or use it in any other way.
* 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.
1. 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 organisations to adopt or maintain processing systems that are technically compatible with other organisations just to satisfy this right.
* 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
1. 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 organisation’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.
1. 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 Stanton Surgery) 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.

Example

The organisation intends to use a new HR system that collates information about employees (unplanned leave, appraisal scores etc) and gives them a performance score. Employees that are not performing well are provided with additional training and support to improve performance and they will not be considered for promotion until their performance score improves.

Before engaging the software, the organisation should speak with their DPO who will ensure that the profiling is fair, lawful and accurate before it can go ahead.

Example

A healthcare provider wants to start using a clinical decision support tool for its patients. The tool will allow them to enter certain data items and then it will produce a score or rating to tell them whether the patient is a high risk for a specific outcome such as contracting COVID or being admitted to hospital.

Before engaging the software, the organisation should speak with their DPO who will ensure that the profiling is fair and lawful before it can go ahead.

1. CHILDREN AND YOUNG PEOPLE
* Young people from aged 12 (and sometimes younger) are allowed to make decisions about how their health information is shared
* A parent or guardian may apply for access to young person's information
* If a young person does raises objections – the parent may not be provided with access to the child’s record
* If the young person does not have the capacity to understand, access may be provided to the parent / carer because it is in the young person's best interest to do so
* Young people can ask you to keep certain parts of their information confidential
* If the young person is making decisions about their information that puts them at risk – we may notify adults with parental rights
* It is important to be open and transparent with Children and Young People about when you can maintain confidentiality and when you cannot.
* Where consent is provided by the Child or Young Person – consider whether this is freely given or provided under pressure from the parent or guardian.
* The young person may not be aware that they can release their record but hide certain items.

Example

Mrs Zajdler has made a Subject Access Request on behalf of her 15-year-old daughter Alicia. Alicia's record has information about contraception and a sexually transmitted disease. Mrs Ahmed confirms that her daughter has provided consent.

Because of her age, Alicia is assumed to have capacity to make decisions about this access.

Consider speaking with Alicia in private to ensure that she is not being pressured and does not want elements of her record redacted.

If Alicia lacks the capacity, assessment should be made around her best interests. There may be elements of the record where, even with fluctuating capacity, Alicia might still reasonably expect confidentiality. Speak with the DPO before release.

Example

Erica, a 14-year-old with a rare condition has expressed an interest in her care record being part of a research project.  Her parents do not want her information to be disclosed.

Because of her age, Erica is expected to have capacity for information sharing. Consider concerns of parents as they might have information you are not aware of (for example, they may have capacity concerns or perhaps the condition is genetic, and her involvement would breach their own confidentiality). Ensure Erica has been provided with age-appropriate privacy materials and fully understands the implications of her decisions – including that she may not be able to change her mind later. If disclosure will take place despite parent’s protest, parents should be notified in advance.  Speak with DPO before release.

1. COMPLAINTS

The practice has a complaints procedure in place that mentions information rights and the person or people managing complaints know when to trigger he involvement of the Data Protection Officer.

If staff receive any complaints related to data protection, they should be forwarded to stanton.surgery@nhs.net.

1. APPLICATION AND AUDIT

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.

* The organisation will list the information rights on our privacy policy
* All staff should be able to recognise and refer information rights requests to the right person
* All staff, visitors and service users should have access to the Data Protection Officer’s contact details to support with rights
* New projects, suppliers or systems must be raised with the Data Protection Officer for review
* The organisation will keep a log of all information rights requests to ensure that we are responding in a consistent and timely way
* Staff must confirm that they have read and understood this protocol
* This protocol will be reviewed annually or sooner in the event of significant learning or change
* This protocol should be read in conjunction with the other protocols in the Data Protection and Security policy suite
* Subject Access Requests are covered in the Disclosures and Access Protocol