Leicestershire Partnership NHS Trust

Individual's Information Rights Policy

This Policy relates to the rights of individuals with regard to their personal data held and processed by the Trust under the new Data Protection legislation.

Key Words:	Data Protection; Individual Rights; Subject Access	
Version:	2	
Adopted by:	Trust Policy Committee	
Date this version was adopted:	7 October 2020	
Name of Author:	Data Privacy Manager	
Name of responsible Committee:	Data Privacy Committee	
Please state if there is a reason for not publishing on website:	n/a	
Date issued for publication:	October 2020	
Review date:	April 2021 (as expecting changes in law following Brexit)	
Expiry date:	1 October 2021	
Target audience:	All staff	
Type of Policy	Clinical ✓	Non Clinical ✓
Which Relevant CQC Fundamental Standards?	Good Governance	

Contents

REFERENCES AND ASSOCIATED DOCUMENTATION

Version Control and Summary of Changes

Version number	Date	Comments (description change and amendments)
1.0	May 2018	This is the first policy under the new General Data Protection Regulation and the UK Data Protection Act 2018. It replaces the Subject Access Policy v4.0 to include the enhanced information rights of individuals under the new legislation.
1.01 Draft	August 2020	Amendments following ICO published guidance and policy review expectation

For further information contact:
Head of Data Privacy

Data Privacy Manager

Data Privacy Officer

Email: LPT-DataPrivacy@leicspart.secure.nhs.uk

Equality Statement

Leicestershire Partnership NHS Trust (LPT) aims to design and implement policy documents that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account the provisions of the Equality Act 2010 and promotes equal opportunities for all. This document has been assessed to ensure that no one receives less favourable treatment on the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity.

Due Regard

LPT will ensure that Due regard for equality is taken and as such will undertake an analysis of equality (assessment of impact) on existing and new policies in line with the Equality Act 2010. This process will help to ensure that:

- **Strategies, policies and services are free from discrimination;**
- **LPT complies with current equality legislation;**
- **Due regard is given to equality in decision making and subsequent processes;**
- **Opportunities for promoting equality are identified.**

Please refer to due regard assessment (Appendix 4) of this policy.

Definitions that apply to this Policy

Automated decision-making	Making a decision solely by automated means without any human involvement.
Caldicott Guardian	Senior person in an NHS organisation responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing.
Controller	A Controller (formerly referred to as Data Controller) determines the purposes and means of processing personal data.
Data Protection Act 2018	The Data Protection Act 2018 (DPA 2018) replaces the UK's Data Protection Act 1998. It applies GDPR standards to domestic UK law that falls outside the scope of European law, e.g. immigration and national security. It also transposes the EU Data Protection Directive 2016/680 (Law Enforcement Directive) into domestic UK law. It is therefore important to read the GDPR and the DPA 2018 side by side.
Data portability	To obtain personal data in a format that allows the data subject to move, copy or transfer their data easily from one IT environment to another in a safe and secure way, without affecting its usability.
Data Protection Officer (DPO)	The DPO is a formally recognised role that is responsible for overseeing data protection strategy and implementation to ensure compliance with data protection legislation requirements.
Data Subject access request	A request by the data subject for copies of their personal data held by the data controller and/or data processor.
Data Subject	A living individual who is the subject of the personal data.
Erasure	The removal of recorded personal data. Also known as 'the right to be forgotten'.
Excessive	This links to 'manifestly unfounded' and relates to requests. The ICO describes a request as being excessive where: • It repeats the substance of previous requests and a reasonable interval has not elapsed • It overlaps with other requests
General Data Protection Regulation (GDPR)	The GDPR is a European law affecting all EU member states and is part of the wider package of reform to the data protection landscape setting out requirements for how organisations need to handle personal data.
Health Professional	A health professional is an individual who provides preventive, curative, promotional or rehabilitative health care services in a systematic way to people, families or communities, e.g.: • Medical Doctors – both Generalist and Specialist Practitioners, including Public Health Doctors • Nursing Professionals, including Public Health Nurses • Pharmacists • Dieticians and nutritionists • Physiotherapists and other therapy-related occupations.

Health Record	A record consisting of information about 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. A health record can be electronic and/or manual form. It may include such documentation as hand written clinical notes, letters to and from health professionals, reports, x-rays and other imaging records, printouts, photographs, video and audio recordings.
Information Commissioner's Officer (ICO)	The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
Information society services	Any service normally provided for remuneration at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, at the individual request of a recipient of the service, e.g. web shops and market places.
Manifestly unfounded	This refers to where are request is deemed 'manifestly unfounded' which is defined by the ICO as: "If the individual has no clear intention to access the information or is malicious in intent and is using the request to harass an organisation with no real purpose other than to cause disruption."
Objection	An expression or feeling of disapproval or opposition by a data subject to the processing of their personal data.
Personal data	Any information relating to an identifiable, living person who can be directly or indirectly identified, particularly by reference to an identifier.
Processor	A processor (formerly known as Data Processor) is responsible for processing personal data on behalf of a Controller, and under instruction from the Controller
Profiling	Automated processing of personal data to evaluate certain things about an individual. Profiling can be part of an automated decision-making process.
Recipient	A natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
Rectification	To have inaccurate personal data corrected, or completed if it is incomplete.
Redact	To permanently delete information prior to disclosure.
Restriction	To prevent further processing of personal data.
Senior Information Risk Owner (SIRO)	The SIRO has board level responsibility for the management of information risk within the Trust and has responsibility for data and cyber security.
Special	Previously known as 'sensitive data' it is data that requires additional protection. Genetic data and some biometric data are included in

category data	the definition. However, it excludes personal data relating to criminal offences and convictions, although these still requires a higher level of protection.
Third party data	Information held within the data subject's records that relates to anyone other than the data subject, data controller, or data processor.
Third Party Request	A subject access request from anyone other than the data subject, data controller, or data processor, e.g. solicitor, data subject's representative acting on their behalf.

1.0. Purpose of the Policy

This Policy provides information about the rights of individuals with regard to their

personal data held and processed by the Trust under Data Protection Legislation (EU General Data Protection Regulation 2016/679 (GDPR) and Data Protection Act 2018 (DPA 2018).

The aim of this policy is to support staff to understand their responsibilities in relation to the information rights of individuals whose personal data they process and to ensure the Trust complies with its legal obligations.

2.0 Summary and Key Points

The GDPR and DPA 2018 enhance the rights of individuals in respect of their own data held by an organisation and includes the following rights:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related automated decision-making, including data profiling

The following provisions apply to all the above information rights:

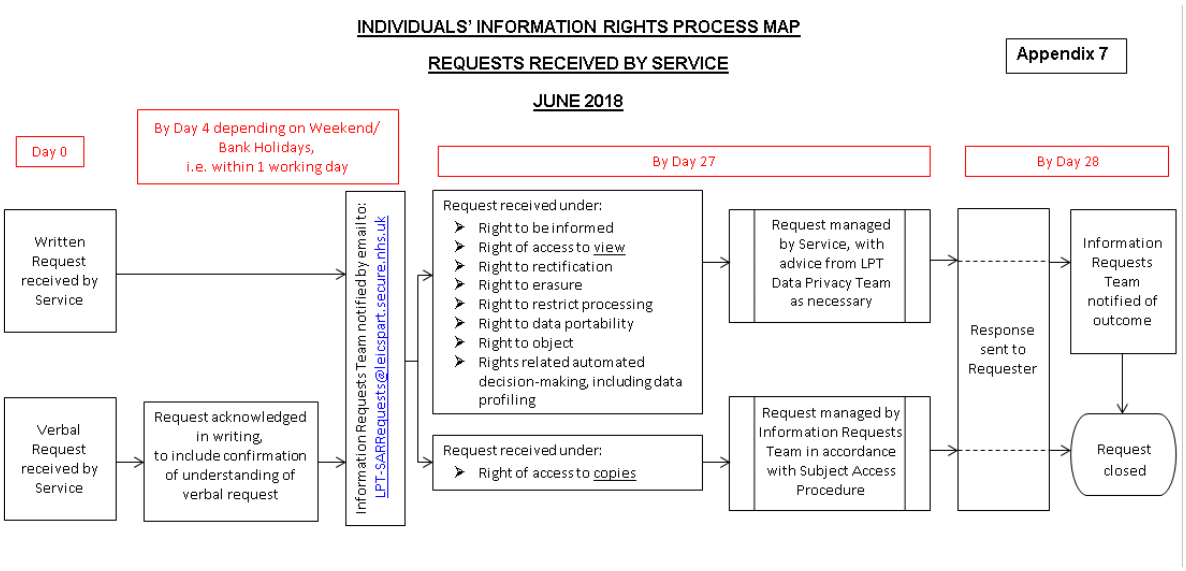
- **Requests can be made verbally or in writing**
- **Requests must be acted upon without undue delay and responded to within one month**.
  For practical purposes and to comply with system requirements a 28-day period has been adopted by the Trust to ensure compliance is always within a calendar month.
- **The identity of the individual needs to be confirmed before disclosing personal data**
- **Most requests are free of charge**

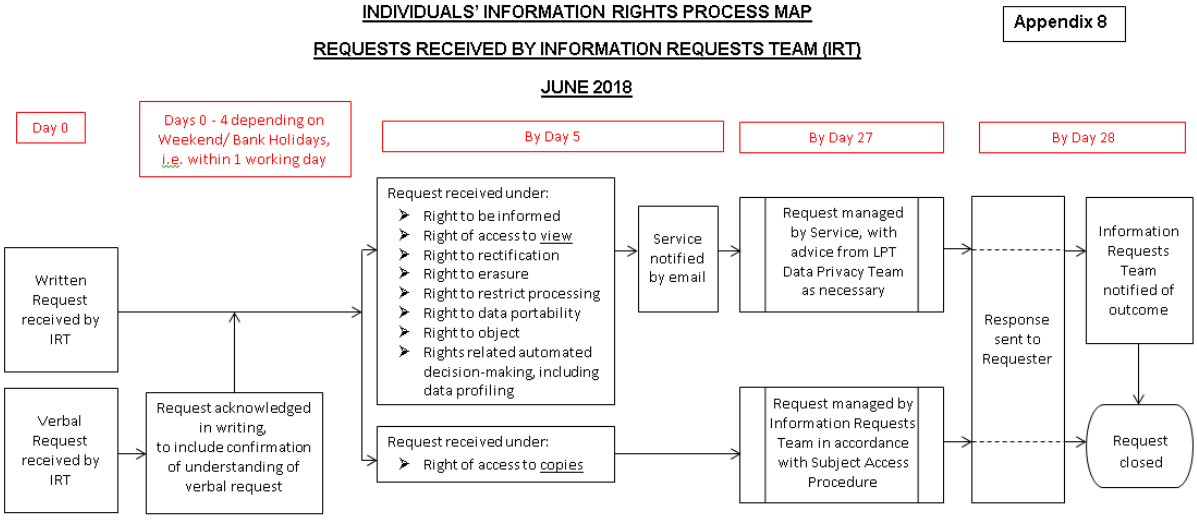
3.0 Introduction

Every member of the Trust, including permanent staff, temporary staff, volunteers, Contractors, Non-Executive Directors and anyone else who works on behalf of the Trust, has a legal obligation to maintain confidentiality and process personal data in accordance with current legislation.

Individuals who come into contact with the Trust have rights under law to ensure their data is kept secure. The GDPR and DPA 2018 enhance the information rights of individuals.

4.0 Requests Flowcharts





5.0. Duties within the Organisation

5.1 **The Trust Board** has a legal responsibility for Trust policies and for ensuring that they are carried out effectively.

5.2 **Trust Board Sub-committees** have the responsibility for ratifying policies and protocols.

5.3 **Caldicott Guardian** is responsible for the strategic management of confidentiality within the organisation and for providing advice on confidentiality issues. The Caldicott Guardian, as guardian of patient data, must approve each new or changed agreement to share personal data with external organisations, such as acute hospitals, social services, police, prisons and private health care. The Caldicott Guardian is responsible for determining a relevant clinician when needed, as well as providing trained resource for screening records, when required, prior to disclosure.

5.4 **Senior Information Risk Owner** is a Trust Board member responsible for overseeing the strategic management of information risks across the organisation.

5.5 **The Head of Data Privacy** undertakes the role of Data Protection Officer, and is responsible for overseeing data protection strategy and implementation to ensure compliance with data protection legislative requirements. Along with the Data Privacy Team they are responsible for providing advice and guidance on data protection issues, including individuals' information rights.

5.4 **Service Directors and Heads of Service** are responsible for:

- Ensuring the contents of this policy are disseminated and discussed, e.g. at staff meetings, and that possible implications for service delivery are identified and acted upon.
- Ensuring staff within their area of responsibility are aware of this policy and comply with its requirements. Services are required to act promptly upon any request by an individual under this policy, whether received verbally or in writing, and to notify the Data Privacy Team without undue delay, so the request can be formally logged and compliance with timescales monitored..
- Ensuring staff understand their responsibility to manage all requests for the following individuals' rights:
  - Right to be informed
  - Right of informal access to view records
  - Right to rectification
  - Right to erasure
  - Right to restrict processing
  - Right to data portability
  - Right to object
  - Rights related automated decision-making, including data profiling
- Ensuring mandatory annual training requirements are met and all staff are compliant.

5.5 **Data Privacy Team** are responsible for:

- Formally logging all requests handled under this policy on the Trust's designated system
- Monitoring compliance against statutory timescales
- Reporting on key performance indicators for compliance
- Managing all formal requests for access, i.e. where copies of records are required
- Managing all requests for records of deceased individuals handled under the Access to Health Records Act 1990.

5.6 **Managers and Line Managers** are responsible for:

- Ensuring staff within their area of responsibility are informed of the contents of this policy.
- Ensuring those staff comply with their legal requirements in relation to the rights of individuals whose data they are processing.
- Ensuring mandatory annual training requirements are met and staff are compliant.

5.7 **All Staff,** whether permanent, temporary, contractors, volunteers, Non-Executive Directors and anyone else who works on behalf of the Trust, are responsible for:

- Maintaining awareness of this policy and any future updates.
- Understanding their responsibilities within its requirements to uphold the rights of individuals in relation to processing personal data.
- Recognising requests in relation to individuals' rights and acting upon them promptly and within statutory timescales.
- Undertaking annual mandatory training, ensuring they remain compliant.
- Reporting via the Trust e-IRF system, any non-compliance with the policy resulting in a failure to uphold individual rights and/or a personal data breach.

6.0 Individuals' Information Rights

The Trust has a legal obligation to identify that an individual has made a request under the following rights and to handle it accordingly:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related automated decision-making, including data profiling

The following provisions apply to all the above information rights:

- **Requests can be made verbally or in writing**
  The individual does not need to specify the exact phrase relating to their request, e.g. 'Right of access' or mention the relevant Article in the GDPR or reference the Data Protection Act. Verbal requests must be recorded and confirmed with the individual to ensure their request has been clearly understood.
- **Requests must be acted upon without undue delay and responded to within one month**.
  The time limit starts from the day after you receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next

month, i.e. the day of receipt is Day 0.

For practical purposes and to comply with system requirements a 28-day period has been adopted by the Trust to ensure compliance is always within a calendar month.

The timescale can be extended by two months where the request is complex and/or numerous. In this instance the individual must be informed of the decision to extend the timescale, as well as the reason why it is necessary, within one month of receiving their request.

- **The identity of the individual needs to be confirmed before disclosing personal data**
  If there are doubts about the identity of the person making the request, proof of ID must be requested. However, the individual must be told without undue delay that more information is needed from them to confirm their identity. The period for responding to the request begins when the identification information is received.

- **Most requests are free of charge**
  Normally, requests will be processed and information provided, where applicable, free of charge.

  Where a request is considered to be 'manifestly unreasonable, unfounded, excessive, or repeated' a reasonable fee, based on the administrative cost only may be charged, or the request refused. In either case the decision will need to be justified. Where a fee is requested the request does not need to be complied with until the fee is received.

- **Refusing a request**
  If a request is refused, the individual must be informed without undue delay and within one month of receipt of the request, including:
- the reason(s);
- their right to make a complaint to the ICO; and
- their ability to seek to enforce this right through a judicial remedy.

6.1 **The Right to be Informed:**

The right to be informed encompasses the obligation to provide clear and concise 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how the Trust uses personal data.

Typically a privacy notice will include:

- the lawful basis for processing the personal data;
- what personal information is held;
- what you do with it and what you are planning to do with it;
- what you actually need;
- whether you are collecting the information you need;
- whether you are creating new personal information;
- who it will be shared with;
- whether there are multiple data controllers;
- the retention periods for the personal data

- the individual's right of access to their information

Also consider including:

- the links between different types of data you collect and the purposes that you use each type of data for;
- the consequences of not providing information;
- what you are doing to ensure the security of personal information; and
- what you will not do with their data.

See Appendix 6 for a copy of the ICO's Privacy Notice Checklist.

- The service must provide privacy information to individuals at the time they collect personal data from them. This is usually part of the service information leaflet.
- If you obtain personal data from other sources, you must provide individuals with a privacy notice within a reasonable period of obtaining the data and no later than one month.
- There are a few circumstances when you do not need to provide people with privacy information, such as if an individual already has the information or if it would involve a disproportionate effort to provide it to them. This is where including the link to the Trust Privacy Notice in the footer of letters assists with meeting this obligation.
- The information you provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.
- It is often most effective to provide privacy information to people using a combination of different techniques including:
  - orally;
  - in writing;
  - through signage; and
  - electronically.

You must regularly review, and where necessary, update your privacy notices. You must bring any new uses of an individual's personal data to their attention before you start the processing.

6.2 The Right of Access

This right is commonly known as a Subject Access Request and gives an individual the right to obtain a copy of the personal data as well as supplementary information such as:

- confirmation whether data about them is being processed
- the purposes for which their data is being processed – this largely corresponds to the information that should be provided in a privacy notice

The information must be provided:

- free of charge, unless 'manifestly unreasonable'.

  Where this is the case a reasonable fee, based on the administrative cost only

of providing the information, may be charged to comply with 'manifestly unreasonable' requests, or requests for further copies of the same information. This does not mean that all subsequent access requests can be charged for;

- within **one month** of receipt (or 3 months if complex/numerous)

Where an individual makes a request to access their own information, either directly or via a third party, e.g. an organisation acting on their behalf, the identity of the person making the request should be verified, using 'reasonable means'.

If the request is made electronically, the information should be provided in a commonly used electronic format.

6.2.1 *The right of access to view personal data – Informal Request*

This is where an individual makes a request to view their health records.

- It is the responsibility of the health professional in charge of the applicant's care to organise an appropriate viewing.
- The applicant must not be allowed to access their health records on his/her own, or to take original records away from Trust property.
- The health professional should arrange suitable representation for the patient to help understand any technical language or medical terminology they may have difficulty understanding in the records.

The same rules apply for an informal as for a formal request. This request will be managed by the service and the request formally logged and monitored by the Trust's Data Privacy Team.

6.2.2 *The right of access to Deceased Patients' records*

This is technically not covered by Data Protection Legislation and therefore not caught by individual's information rights. Requests relating to applications to access information held about deceased individuals continue to fall under the Access to Health Records Act 1990.

The Trust is responsible for the confidentiality of patient information after a patient's death. As such, the need to maintain the individual's confidentiality remains with the Trust in the absence of the patient's consent.

The Access to Health Records Act 1990 restricts access to records compiled on or after the 1st November 1991. Therefore, there is no right of access to information compiled prior to this date.

The 1990 Act provides for an application to be submitted by:

 the patient's personal representative, and

 by any person who may have a claim arising out of the patient's death.

In line with the data protection legislation the right to access personal data is normally free of charge. The Trust has, therefore, decided to adopt the same approach for access to a deceased person's record.

6.2.2.1 ***The personal representative***

The personal representative is the only person who has an unqualified right of access to a deceased person's record and need give no reason for applying to access that record.

He/she will either be an executor for the estate of a deceased person who left a Will, or the administrator of a deceased person who died intestate (without a Will). In either case a court will issue "letters testamentary", "letters of administration" or "letters of representation" stating that an executor or administrator has been appointed. This proof of authority plus a copy of the deceased's death certificate will be required prior to processing such a request, together with the proof of identity of the personal representative is required.

More detailed guidance on the processing of requests for access can be found in the Subject Access Requests Procedure.

6.3 The Right to Rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. Personal data is defined under DPA18 as inaccurate if it is factually incorrect or misleading as to any matter of fact.

As with all other types of individual information rights requests, an individual can make a request for rectification verbally or in writing. Verbal requests must be recorded and confirmed with the individual to ensure their request has been clearly understood.

A request to rectify personal data does not need to mention the phrase 'request for rectification' or Article 16 of the GDPR to be a valid request. As long as the individual has challenged the accuracy of their data and has asked for it to be corrected, or has asked that you take steps to complete data held about them that is incomplete this will be a valid request.

If a request for rectification is received all reasonable steps should be taken to be satisfied that the data is accurate and to rectify the data if necessary.

An individual has the right to request restriction of the processing of their personal data where they contest its accuracy and this is being checked. As a matter of good practice, processing of the personal data in question should be restricted whilst its accuracy is being verified, whether or not the individual has exercised their right to restriction.

This request will be managed by the service and the request formally logged and monitored by the Trust's Data Privacy Team.

6.3.1 ***Considerations***

When considering the individuals request, all arguments and evidence provided by the data subject should be taken into account. What steps are reasonable will depend, in particular, on the nature of the personal data and what it will be used for. The more important it is that the personal data is accurate, the greater the effort necessary to check its accuracy and, if required, the steps taken to rectify it.

For example, greater effort should be made to rectify inaccurate personal data if it is used to make significant decisions that will affect an individual or others, rather than trivial ones. Steps already taken to verify the accuracy of the data prior to the challenge by the data subject should also be taken into account.

Determining whether personal data is inaccurate can be more complex if the data refers to a mistake that has subsequently been resolved. It may be possible to argue that the record of the mistake is, in itself, accurate and should be kept. In such circumstances the fact that a mistake was made as well as the correct information should be included in the individual's data.

Where the data in question records an opinion, this can be complex. Opinions are, by their very nature, subjective, and it can be difficult to conclude that the record of an opinion is inaccurate. As long as the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is, it may be difficult to say that it is inaccurate and needs to be rectified. Where rectification is refused on these grounds, the individual's disagreement with the opinion should nevertheless be recorded.

It is good practice to place a note on the system/record indicating that the individual challenges the accuracy and the reasons for this. This is commonly known as an Addendum to the record.

6.3.2 ***Actions to be taken***

- If the personal data in question has been disclosed to third parties, they must be informed of the rectification where possible.
- The 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.

6.3.3 ***Refusing A Request***

A request for rectification can be refused if the request is manifestly unfounded or excessive (see policy definitions), taking into account whether the request is repetitive in nature.

If a request is considered manifestly unfounded or excessive it is possible to:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case the decision will need to be justified.

The reasonable fee should be based on the administrative costs only of complying with the request. If a decision is taken to charge a fee the individual must be contacted without undue delay and within one month. The request does not need to be complied with until the fee has been received.

Where a request for rectification is refused, the reason why must be explained to the individual, informing them of their right to complain to the Information Commissioner's Office and to a judicial remedy.

6.4 The Right to Erasure

The right to erasure is also known as 'the right to be forgotten'. The right is not absolute and **only applies in certain circumstances.**

It should be noted that this right <u>does not</u> apply to information held for the provision of direct care.

Where information collected is not used for direct care purposes, for example, for teaching and publication, this request will be managed by the service and the request formally logged and monitored by the Trust's Data Privacy Team.

The broad principle underpinning 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, for example, where the personal information is no longer necessary to fulfil the purposes for which it was collected.

Individuals can make a request for erasure **verbally or in writing** and do not need to include the phrase 'request for erasure'. Where a verbal request is received this must be logged formally and acted upon promptly by the service.

6.4.1 ***Considerations***

This right is not limited to processing that causes unwarranted and substantial damage or distress. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

6.4.2 ***Action to be taken***

- Requests must be responded to within **one month.**
- Recipients must be notified if any data is erased that we have shared with them.

6.4.3 ***Exemption***

There are some specific circumstances where the right to erasure does not apply and you can refuse to deal with a request. The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation; **the right to erasure does not apply to health records, where a complete audit trail must be preserved.**
- for the performance of a task carried out in the public interest or in the exercise of official authority - **the right to erasure does not apply to health records as provision of healthcare is a public task**
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing – **the right of erasure does not apply to health research**; or
- for the establishment, exercise or defence of legal claims.

Data Protection Legislation also specifies two circumstances where the right to erasure will not apply to special category (sensitive) data:

- if the processing is necessary for public health purposes in the public interest (eg protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices) **Public health screening and pandemic management**; or
- if the processing is necessary for the purposes of preventative or occupational medicine (eg where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (eg a health professional). **This is the health records exemption**

6.5 The Right to Restrict Processing

Individuals have a right to request restriction or suppression of processing their personal data. This is not an absolute right and applies in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data. This request will be managed by the service and the request formally logged and monitored by the Trust's Data Privacy Team.

An individual can make a request for restriction **verbally or in writing.**

Processing includes a broad range of operations including collection, structuring, dissemination and erasure of data. Methods used to restrict the processing should be appropriate for the type of processing being carried out.

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information held or how it has been processed. In most cases the restriction of an individual's personal data will only be in place for a certain period of time and not indefinitely.

Individuals have the right to request restriction of the processing of their personal data in the following circumstances:

- the individual contests the accuracy of their personal data and therefore processing is restricted whilst the accuracy is being verified;
- the data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;
- the personal data is no longer needed, but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or
- the individual has exercised their right to object to the processing of their data under Article 21(1), i.e. either:
- where 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; or
- where processing is necessary for the purposes of **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, and you are considering whether your legitimate grounds override those of the individual.

As a matter of good practice processing should automatically be restricted whilst its accuracy or the legitimate grounds for processing the personal data in question is being considered.

6.5.1 ***Actions to be taken***

When processing is restricted:

- The personal data may be stored, but not processed further;
- Enough information about the individual can be retained to ensure that the restriction is respected in future;
- Individuals must be informed when a decision is taken to lift a restriction on processing, **before** the restriction is lifted;
- The request must be responded to within **one calendar month**. This can be extended by a further two months if the request is complex a number of requests have been from the individual. The individual must be informed of the reason for the extension within one month of receiving their request.
- 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.

The restricted data must not be processed in any way **except to store it** unless:

- the individual consents to the processing;
- it is for the establishment, exercise or defence of legal claims;
- it is for the protection of the rights of another person (natural or legal); or
- it is for reasons of important public interest.

6.5.2 ***Methods***

A number of different methods can be used to restrict data, such as:

- temporarily moving the data to another processing system;
- making the data unavailable to users; or
- temporarily removing published data from a website.

If an automated filing system is being used, technical measures will be required to ensure that any further processing cannot take place and that the data cannot be changed whilst the restriction is in place. A note should also be placed on the system that the processing of this data has been restricted.

6.5.3 ***Refusing a Request***

A request for restriction can be refused if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

6.6 The Right to Data Portability

This right is new under Data Protection Legislation. It is limited to information that is held in a machine readable format. **N.B: personal data processed by the Trust under its legal obligations to provide healthcare services is excluded from the right to Data Portability**

This right does apply to telephone/video recordings, including CCTV footage, where it exists.

A request under this right will be managed by the service and the request formally logged and monitored by the Trust's Data Privacy Team.

The right to 'Data Portability' only applies:

- to personal data an individual has provided to a Controller, i.e. data derived, inferred or created by the Controller is excluded;
- 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, i.e. paper records are excluded.

6.7 The Right to Object

This request will be managed by the service and the request formally logged and monitored by the Trust's Data Privacy Team. Individuals who have an objection on "grounds relating to his or her particular situation" have the right to stop or prevent processing.

This request will be managed by the service and the request formally logged and monitored by the Trust's Data Privacy Team.

This right only applies in certain circumstances:

1. Absolute right – Direct Marketing
2. Not Absolute – Task carried out in the public interest; Exercise of official duty; Legitimate interests
3. More Limited - Scientific/historical research/statistical purposes

6.7.1 ***Not Absolute***

The individual must give reasons for objecting and based on their particular situation. However as this is **not** an absolute right, the request can be refused if:

- there are compelling legitimate grounds 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;
- where the processing of personal data is for the purposes of research and is necessary for the performance of a public interest task.

6.7.2 ***Considerations***

- Individuals reasons particularly where there is substantial damage or distress (e.g. processing causing financial loss) where their grounds for objection may have greater weight

- Balance the individuals interests, rights and freedoms, remembering the responsibility to demonstrate the legitimate grounds to override those of the individual.

6.7.3 ***Research***

Processing for these purposes with the appropriate safeguards (data minimisation/pseudonymisation), the individual only has the right to object if the lawful processing is:

- Public task/exercise of official duty
- Legitimate interests

The individual **does not** have the right to object if the lawful basis is public task necessary for the performance of a task carried out in the public interest.

6.8 The Right not to be subject to Automated Decision-making including Profiling.

The GDPR has provisions on:

- automated individual decision-making (making a decision solely by automated means without any human involvement). For example, a recruitment aptitude test which uses pre-programmed algorithms and criteria; and
- profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

The GDPR applies to all automated individual decision-making and profiling.

Article 22 of the GDPR has additional rules to protect individuals where an organisation carries out solely automated decision-making that has legal or similarly significant effects on them. This type of decision-making can only be undertaken where the decision is:

- necessary for the entry into or performance of a contract; or
- authorised by Union or Member state law applicable to the controller; or
- based on the individual's explicit consent.

Because this type of processing is considered to be high-risk the GDPR requires a Data Protection Impact Assessment to be carried out show that risks have been identified, assessed what actions are necessary to address them.

As well as restricting the circumstances in which automated decision-making can be made the GDPR also:

- requires individuals to be given specific information about the processing;
- obliges steps to be taken to prevent errors, bias and discrimination;
- gives individuals rights to challenge and request a review of the decision;

These provisions are designed to increase individuals' understanding of how you might be using their personal data.

A request under this right will be managed by the service and the request formally

logged and monitored by the Trust's Data Privacy Team.

NB The Trust does not currently use personal and/or sensitive (special category) information to make decisions without the intervention of a person, be that a health professional or authorised member of staff

7.0 Failure to Comply with Individuals' Information Rights

In addition to monetary penalties, the GDPR gives the ICO a suite of sanctions to help organisations comply – warnings, reprimands, corrective orders. While these do not impose financial penalties, an organisation's reputation may suffer significantly.

If a fine is imposed by the ICO, it may be up to a maximum of £17 million or 4% of the turnover, whichever is higher.

The GDPR also gives individuals the right to compensation of any material and/or non-material damages resulting from an infringement of the GDPR.

When deciding whether to impose a fine and the level, the ICO must consider:

- The nature, gravity and duration of the infringement;
- The intentional or negligent character of the infringement;
- Any action taken by the organisation to mitigate the damage suffered by individuals;
- Technical and organisational measures that have been implemented by the organisation;
- Any previous infringements by the organisation or data processor;
- The degree of cooperation with the regulator to remedy the infringement;
- The types of personal data involved;
- The way the regulator found out about the infringement;
- The manner in which the infringement became known to the supervisory authority, in particular whether and to what extent the organisation notified the infringement;
- Whether, and, if so, to what extent, the controller or processor notified the infringement; and
- Adherence to approved codes of conduct or certification schemes.

8.0 Training needs

There is a need for training identified within this policy. In accordance with the classification of training outlined in the Trust Learning and Development Strategy this training has been identified as mandatory training.

At least 95% of all staff, including new starters, locums, temporary, students and staff contracted to work in the organisation must have completed their annual Data Security Awareness Level One training in the period 1 April to 31 March. A record of the training will be recorded on uLearn.

The information button  against the title of the module 'NHS Data Security Awareness Level 1' on uLearn identifies who the training applies to, the update frequency and learning outcomes.

There is also a recommendation for additional non-mandatory subject specific training where roles involve the management of requests to access health records.

The governance group responsible for monitoring the training is Trust's Data Privacy Committee.

9.0 Monitoring Compliance and Effectiveness

9.1 **Individuals' Rights**
Performance figures relating to numbers of requests, the average turnaround times and compliance rates for statutory timescales are provided on a monthly basis as part of the Trust's Performance Report presented to the Trust Board.

Regular reports to the Trust's Data Privacy Committee provide analysis of how requests managed under data protection legislation have been handled and monitor performance against statutory timescales. An annual report is also provided to the group at the end of each year.

Ref	Minimum Requirements	Evidence for Self-assessment	Process for Monitoring	Responsible Individual / Group	Frequency of monitoring
9.1	Requests to be responded to within statutory timescale	Section 2.1	Performance report to Trust Board	Trust Board	Monthly
9.1	Requests to be responded to within statutory timescale	Section 2.1	Information Requests Report	Data Privacy Committee	2-3 times per year, plus annual report at end of year
9.2	At least 95% of all staff, including new starters, locums, temporary, students and staff contracted to work in the organisation must have completed their annual Data Security Awareness Level One training in	Section 6.0	Managers and Line Managers to monitor compliance within their area of responsibility.	Data Privacy Committee	Bi-monthly

Ref	Minimum Requirements	Evidence for Self-assessment	Process for Monitoring	Responsible Individual / Group	Frequency of monitoring
	the period 1 April to 31 March.				

10.0. Standards/Performance Indicators

TARGET/STANDARDS	KEY PERFORMANCE INDICATOR
Data Security and Protection Toolkit Data Security Standard 3 All staff complete appropriate annual data security training and pass a mandatory test. The training includes a number of realistic and relevant case studies.	At least 95% of all staff, including new starters, locums, temporary, students and staff contracted to work in the organisation must have completed their annual Data Security Awareness Level One training in the period 1 April to 31 March.

11.0 References and Bibliography

The policy was drafted with reference to the following:

- Information Commissioner's Office Guide to the General Data Protection Regulation, March 2018
- Information Governance Alliance General Data Protection Regulation (GDPR) guidance
- GDPR recitals and articles
- Data Protection Act 2018
- Subject Access Requests Procedure

Appendix 1

Training Requirements
There is a need for training identified within this policy. In accordance with the classification of training outlined in the Trust Learning and Development Strategy this training has been identified as mandatory training.

At least 95% of all staff, including new starters, locums, temporary, students and staff contracted to work in the organisation must have completed their annual Data Security Awareness Level One training in the period 1 April to 31 March. A record of the training will be recorded on uLearn.

The information button  against the title of the module 'NHS Data Security Awareness Level 1' on uLearn identifies who the training applies to, the update frequency and learning outcomes.

There is also a recommendation for additional non-mandatory subject specific training where roles involve the management of requests to access health records.

The governance group responsible for monitoring the training is Trust's Data Privacy Steering Group.

Training Needs Analysis

Training topic:	Data Security Awareness Level 1 (Mandatory) Access to Health Records (Recommended)
Type of training: (see study leave policy)	√ Mandatory (must be on mandatory training register) √ Role specific ☐ Personal development
Division(s) to which the training is applicable:	√ Adult Mental Health & Learning Disability Services √ Community Health Services √ Enabling Services √ Families Young People Children √ Hosted Services
Staff groups who require the training:	All staff groups are required to undertake the mandatory training annually All staff whose role involves the management of subject access requests are recommended to complete the non-mandatory 'Access to Health Records' training.
Regularity of Update requirement:	Annual
Who is responsible for delivery of this training?	Learning & Development
Have resources been identified?	This supersedes the current Information Governance Basic training
Has a training plan been agreed?	Not applicable, as this supersedes training currently in place
Where will completion of this training be recorded?	√ ULearn ☐ Other (please specify)
How is this training going to be monitored?	Monthly reports

Appendix 2

The NHS Constitution

The NHS will provide a universal service for all based on clinical need, not ability to pay. The NHS will provide a comprehensive range of services

Shape its services around the needs and preferences of individual patients, their families and their carers	☐
Respond to different needs of different sectors of the population	☐
Work continuously to improve quality services and to minimise errors	☐
Support and value its staff	√
Work together with others to ensure a seamless service for patients	☐
Help keep people healthy and work to reduce health inequalities	☐
Respect the confidentiality of individual patients and provide open access to information about services, treatment and performance	√

Appendix 3

Stakeholders and Consultation

Key individuals involved in developing the document

Name	Designation
Sam Kirkland	Head of Data Privacy
Mary Stait	Data Privacy Manager

Circulated to the following individuals for comment

Name	Designation
Members of the Trust Data Privacy Committee	
Dr Avinash Hiremath	Medical Director / Caldicott Guardian
Dr Anne Scott	Chief Nurse
Members of the Data Privacy Team	

Appendix 4

Due Regard Screening Template

Section 1	
Name of activity/proposal	Individuals' Information Rights' Policy
Date Screening commenced	04/08/2020
Directorate / Service carrying out the assessment	Data Privacy Team Finance, Business and Estates
Name and role of person undertaking this Due Regard (Equality Analysis)	Sam Kirkland Head of Data Privacy
Give an overview of the aims, objectives and purpose of the proposal:	
AIMS: To demonstrate compliance with Individuals Information Rights as set out by Data Protection Legislation	
OBJECTIVES: All individuals have a legal right to make information rights requests to the Trust under its statutory obligations as a Controller	

Section 2	
Protected Characteristic	**If the proposal/s have a positive or negative impact please give brief details**
Age	Positive - as does not have an age restriction
Disability	Positive – as is not predicated on ones physical ability and mechanisms have been put in place to ensure that the request process is accessible
Gender reassignment	Neutral
Marriage & Civil Partnership	Neutral
Pregnancy & Maternity	Neutral
Race	Neutral
Religion and Belief	Neutral
Sex	Positive as is not predicated on gender
Sexual Orientation	Neutral
Other equality groups?	None

Section 3			
Does this activity propose major changes in terms of scale or significance for LPT? For example, is there a clear indication that, although the proposal is minor it is likely to have a major affect for people from an equality group/s? Please <u>tick</u> appropriate box below.			
Yes		No	
High risk: Complete a full EIA starting click here to proceed to Part B		Low risk: Go to Section 4.	**No**

Section 4			
If this proposal is low risk please give evidence or justification for how you reached this decision:			
The policy supports individuals' information rights regardless of any personal characteristic.			
Signed by reviewer/assessor	*Sam Kirkland*	**Date**	04/08/2020
Sign off that this proposal is low risk and does not require a full Equality Analysis			
Head of Service Signed		**Date**	

Appendix 5

PRIVACY IMPACT ASSESSMENT SCREENING

Privacy impact assessment (PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individual's expectations of privacy. The first step in the PIA process is identifying the need for an assessment.

The following screening questions will help decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise and requires senior management support, at this stage the Head of Data Privacy must be involved.

Name of Document:	**Individuals' Information Rights Policy**		
Completed by:	**Mary Stait**		
Job title:	**Data Privacy Manager**	**Date**	**31/05/2018**

	Yes / No
1. Will the process described in the document involve the collection of new information about individuals? This is information in excess of what is required to carry out the process described within the document.	**No**
2. Will the process described in the document compel individuals to provide information about themselves? This is information in excess of what is required to carry out the process described within the document.	**Yes**
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information as part of the process described in this document?	**No**
4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	**No**
5. Does the process outlined in this document involve the use of new technology which might be perceived as being privacy intrusive? For example, the use of biometrics.	**No**
6. Will the process outlined in this document result in decisions being made or action taken against individuals in ways which can have a significant impact on them?	**No**
7. As part of the process outlined in this document, is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For examples, health records, criminal records or other information that people would consider to be particularly private.	**No**
8. Will the process require you to contact individuals in ways which they may find intrusive?	**No**

If the answer to any of these questions is 'Yes' please contact the Head of Data Privacy
Tel: 0116 2950997 Mobile: 07825 947786
Lpt-dataprivacy@leicspart.secure.nhs.uk
In this case, adoption of a procedural document will not take place until approved by the Head of Data Privacy.

IG Manager approval name:	**Sam Kirkland**
Date of approval:	**1 June 2018**

Acknowledgement: Princess Alexandra Hospital NHS Trust

Your privacy notice checklist

What?

Decide what to include by working out:

- what personal information you hold;
- what you do with it and what you are planning to do with it;
- what you actually need;
- whether you are collecting the information you need;
- whether you are creating new personal information; and
- whether there are multiple data controllers.

If you are relying on consent, you should:

- display it clearly and prominently;
- ask individuals to positively opt-in;
- give them sufficient information to make a choice;
- explain the different ways you will use their information, if you have more than one purpose;
- provide a clear and simple way for them to indicate they agree to different types of processing; and
- include a separate unticked opt-in box for direct marketing.

Also consider including:

- the links between different types of data you collect and the purposes that you use each type of data for;
- the consequences of not providing information;
- what you are doing to ensure the security of personal information;
- information about people's right of access to their data; and
- what you will not do with their data.

Where?

Give privacy information:

- orally;
- in writing;
- through signage; and
- electronically.

Consider a layered approach:

- just in time notices;
- video;
- icons and symbols; and
- privacy dashboards.

ico.
Information Commissioner's Office

When?

Actively give privacy information if:

- you are collecting sensitive information;
- the intended use of the information is likely to be unexpected or objectionable;
- providing personal information, or failing to do so, will have a significant effect on the individual; or
- the information will be shared with another organisation in a way that individuals would not expect.

How?

Write and present it effectively:

- use clear, straightforward language;
- adopt a style that your audience will understand;
- don't assume that everybody has the same level of understanding as you;
- avoid confusing terminology or legalistic language;
- draw on research about features of effective privacy notices;
- align to your house style;
- align with your organisation's values and principles;
- be truthful. Don't offer people choices that are counter-intuitive or misleading;
- follow any specific sectoral rules;
- ensure all your notices are consistent and can be updated rapidly; and
- provide separate notices for different audiences.

Test and review

Before roll out:

- test your draft privacy notice with users; and
- amend it if necessary.

After roll out:

- keep your privacy notice under review;
- take account of any complaints about information handling; and
- update it as necessary to reflect any changes in your collection and use of personal data.

ico.
Information Commissioner's Office