Information Request Policy

(Previously known as the IG04 Access to Records Policy and IG05 Freedom of Information Policy)

Solent NHS Trust policies can only be considered to be valid and up-to-date if viewed on the intranet. Please visit the intranet for the latest version.

Purpose of Agreement	The purpose of this policy is to ensure all Solent Staff, Contractors and other third parties are aware of their responsibilities, with regards to ensure the Trust's compliance with Legislation, with regards to requests for information
Document Type	[x] Policy
Reference Number	Solent NHST/Policy/ IG22 Previous policies: IG04 and IG05
Version	V1
Name of Approving Committees/Groups	Policy Steering Group Assurance Committee
Operational Date	May 2019
Document Review Date	May 2022
Document Sponsor (Job Title)	Chief Operating Officer and Senior Information Risk Owner
Document Manager (Job Title)	Data Protection Officer and Head of Information Governance & Security
Document developed in consultation with	Information Governance Team
Intranet Location	Policies and Procedures – Solent
Website Location	Policies and Procedures – Publication Scheme
Keywords (for website/intranet uploading)	Subject Access Requests, SAR, Freedom Of Information Requests, FOI, Information Requests

Amendments Summary:

Please fill the table below:

Amend No	Issued	Page	Subject	Action Date

Review Log:

Include details of when the document was last reviewed:

Version Number	Review Date	Lead Name	Ratification Process	Notes
1	08/04/2019	Sadie Bell, DPO Katie Smith, Senior IG Officer & Ass. DPO	-	This policy has been produced by amalgamating similar policies and has been updated to reflect current Data Protection Legislation and Freedom of Information Legislation. Previous policies are; Access to Records Policy FOI Policy FOI Procedures

SUMMARY OF POLICY

This policy outlines how the Trust will meet its legal obligations to process information requests, that fall under Data Protection Legislation, Access to Records Act, Freedom of Information Act and Environmental Information Regulations.

The Trust has taken a decision to centralise the processing of these requests within the Trust's Information Governance Team

All requests for information should be sent to the Information Governance Team to process.

The Information Governance Team should ensure that it maintains expert knowledge in all legislation pertaining to requests for information, covered by this policy. They must also ensure that they review all responses / releases to ensure only appropriate information is released and it is only released to those who are legally entitled to it.

Individual sign-off processes have been identified, as well as processes that should be followed to ensure that requests are compliant with the mandated timescales to release information. The can be found in the appendices of this policy.

.

All staff who are required to sign off the release of information, will be fully supported and guided by the Information Governance Team

Table of Contents

1 Introduction & Purpose

1.1 Solent NHS Trust has a legal obligation to comply with all appropriate legislation in respect of the information it processes and publishes. This policy covers the request and release processes for information requested under; Freedom of Information Act 2000, Environmental Information Act 2004, the Re-use of Public Sector Information, and all current Data Protection legislations.

1.2 This policy has been written to assist all staff with a responsibility for dealing with requests for personal data to include; patient/client records, x-rays, occupational health, personnel information in all formats (paper/electronic), photographs, videos and tape recordings of telephone conversations are all known as Subject Access Requests (SAR) and for dealing with requests for non-personal data to include; business, financial, performance or environmental information, this list is not exhaustive known as Freedom of Information Requests (FOI) or Environmental Information Requests (EIR).

1.3 This policy outlines how the Trust will ensure that it complies with (but not limited to) the following;

- Freedom of Information Act 2000
- Public Records Acts 1958 and 1967
- Environmental Information Act 2004
- Access to Health Records Act 1990 (for deceased persons)
- Data Protection Legislations (Subject Access and Police requests)

2 Scope

2.1 This policy applies to bank, locum, permanent and fixed term contract employees (including apprentices) who hold a contract of employment or engagement with the Trust, and secondees (including students), volunteers (including Associate Hospital Managers), Non-Executive Directors, governors and those undertaking research working within Solent NHS Trust, in line with Solent NHS Trust's Equality, Diversity and Human Rights Policy. It also applies to external contractors, Agency workers, and other workers who are assigned to Solent NHS Trust.

2.2 Solent NHS Trust is committed to the principles of Equality and Diversity and will strive to eliminate unlawful discrimination in all its forms. We will strive towards demonstrating fairness and Equal Opportunities for users of services, carers, the wider community and our staff.

3 Definitions

- **Data:** Information which;
  - is being processed by means of equipment operating automatically in response to instructions given for that purpose.
  - is recorded with the intention that it should be processed by means of such equipment,
  - is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system or,
  - does not fall within above paragraph but forms part of an accessible record
- **Personal Identifiable Data (PID):** Means data which relates to an individual who can be identified from the data. This is not just name and address but also information such as; (this list is not exhaustive)

- Data of birth (when used with other identifiers)
- National Insurance Number
- Credit card number
- Passport number
- DNA
- Post code

- **Requestor:** Throughout this document the term 'requestor' is used. This term refers to all individuals or organisations requesting information under these legislations.
- **Processing:** Processing means obtaining, recording or holding the data or carrying out any operation or set of operations
- **Relevant Filing System:** A structured set of information that can reference individuals either directly or indirectly.
- **Third Party** Any person other that the Data Subject, Data Controller or Data Processor
- **Data Subject:** This is the living individual who is the subject of the personal information
- **Data Controller:** A person that collects personal data and who determines the purpose for which, and the manner in which, personal information is to be processed. This may be an individual or an organisation (e.g. Solent NHS Trust) and the processing may be carried out, alone, jointly or in common with other persons.
- **Health Care Professional:** An individual with the relevant knowledge and experience in specific health services.
- **Information Asset Custodian:** A nominated person within services that directly supports the implementation of Information Governance within the Trust.
- **Information Asset Owner:** Senior managers involved in running the business. They should understand and address risks to the information assets they 'own' and provide assurance to the SIRO on the security and use of the assets.
- **Public Interest Test:** A test required to be undertaken once a 'qualified exemption' under FOI or EIR has been applied which weighs the public interest in maintaining the exemption against the public interest in disclosure.
- **Absolute exemption:** Applied information that does not have to be released to the applicant. Absolute exemptions do not require a public authority to undertake a prejudice or public interest test.
- **Qualified exemption:** An exemption that requires a public authority to undertake a public interest test.
- **Duty to confirm or deny:** Any person making a request for information is entitled to be informed by the authority if the information is held or not.
- **Fees Notice:** A written notification issued to an applicant stating that a fee is payable
- **Fees Regulations:** National regulations that will prohibit a fee with regard to certain types of requests, set an upper limit on amounts that may be charged and prescribe the manner in which fees are calculated.
- **Information Commissioner:** The Information Commissioner enforces and oversees Data Protection regulations, Freedom of Information and Environmental Regulation requests. The Commissioner is a United Kingdom (UK) independent supervisory authority reporting directly to the UK Parliament and has an international role as well as a national one. In the UK the Commissioner has a range of duties including the promotion of good information handling and the encouragement of codes of practice for data controllers, that is, anyone who decides how and why personal data, (information about identifiable, living individuals) are processed.

Glossary

DPA	Data Protection Act
DPO	Data Protection Officer

FOI	Freedom of Information
HCP	Health Care Professional
GDPR	General Data Protection Regulations
IAC	Information Asset Custodian
IAO	Information Asset Owner
PID	Personally Identifiable Data
SAR	Subject Access Request
SIRO	Senior Information Risk Owner

4 Requests for Information

4.1 There are number of different types of requests for information, under legislation; this policy outlines how to process each type of request.

4.2 It is important to note that it does not matter what type of request the information being requested falls under, all requests for information should be processed by the Trust's Information Governance Team.

4.3 This policy will outline the Trust's legal requirements and staff requirements to comply with these legal requests. The Information Governance Team will be responsible for implementing internal processes, to assist with the logging, processing and responding to requests, to ensure the Trust's legal compliance.

5 Subject Access Requests

5.1 Requests for living individuals records (health and personnel) are covered under the Data Protection Legislation.

5.2 Individuals have a right to:

- Be informed whether personal data is processed (which includes being held or stored)
- A description of the data held, the purposes for which it is processed and to whom the data may be disclosed
- A copy of the information constituting the data
- Information as to the source of the data
- Where there are multidisciplinary teams working across health and social services boundaries, permission should be sort from each respective body prior to disclosure of records.

5.3 A request should be made in writing, which includes by email, to the data controller. However, where an individual is unable to make a written request it can be made verbally, with the details recorded on the individual's file.

5.4 Any requests received by the Trust should be sent to or forwarded immediately to the Information Governance Team InformationGovernanceTeam@solent.nhs.uk who will log all requests on a central log; allocating a reference number to the request, conducting the necessary checks and being the central point for all communications; including acknowledgements, requests for further information and releases.

5.5 **Checks**

- **Identity**: to comply with the law, information relating to the individual must only be

disclosed to them or someone with their written consent to receive it.

- ✓ Valid Passport
- ✓ Driving Licence
- ✓ Birth Certificate along with some other proof of address, e.g. a named utility bill or a Medical Card.

- **Authority to disclose**: The individual's consent must accompany the request. Solicitors often apply on the individual's behalf; ensure the written authority is attached. Health Care Professionals (HCP) must consider the request and determine whether full, limited or no access should be given (if request could damage mental or physical health of the individual or a third party). Reasons for non-disclosure must be documented, as a Court Order may be sought by the individual or their representative. Copies must be provided; originals should never leave the organisation. If supervised access, this must be by someone competent to explain the contents and terminology to the individual/representative.
- **Consent Issues**: Where an adult lacks capacity, consideration should also be given in respect to the Mental Capacity Act 2005 the HCP must satisfy themselves that an adult lacks capacity and that disclosure would be in the individual's best interests. The principles of access to records are similar to those in respect of Consent to Treatment
- **Lasting Power of Attorney replaced Enduring Power of Attorney on 1st October 2007**: A lasting power of attorney is a legal document that lets a person appoint someone they trust as an 'attorney' to make decisions on their behalf.
  It can be drawn up at any time while a person has capacity, but has no legal standing until it is registered with the Office of the Public Guardian.
  A registered LPA can be used at any time, whether the person has the mental ability to act for themselves or not. There are two types of LPA:
  - ✓ Property and Affairs LPA
  - ✓ Personal Welfare LPA
- **Enduring Power of Attorney (EPA):** A person given power under an EPA before 1 October 2007 can still use it and apply to have it registered. This person has a duty to apply to register the EPA as soon as they believe that a person is becoming or has become mentally incapable of making financial decisions for themselves.
  If a person has an unregistered EPA and still has the capacity to make decisions for themselves, then they can make a Personal Welfare LPA to run alongside it.

Where an access request has previously been met Legislation permits that a subsequent identical or similar request does not have to be fulfilled unless a reasonable time interval has elapsed between. A check will be made of previous requests to ensure that a 'reasonable' time has elapsed since any previous request from the same individual. Although 'reasonable' is not specified in the Act, the nature of the data, the purpose and frequency for which it is used must be considered.

5.6 As good practice the data controller (Solent NHS Trust) may check with the applicant whether all or just some of the information contained in the health record is required before processing the request. This may decrease the cost for the applicant and eliminate unnecessary work by NHS staff. However, there is no requirement under the Act for the applicant to inform the data controller of which parts of their health record they require.

5.7 **Collating Responses**

The IG Team will collate the information, liaise with the relevant service(s) IAC(s) to locate locally held records and prepare the disclosure response to the request as necessary.

If applicable a 'NO RECORDS FOUND' response can be sent.

The IG Team will review the content of the records to ensure that only appropriate information is being released.

Should information be contained in the record that can identify another individual then that should be withheld, unless either of the following circumstances applies:

- the other individual has consented to the disclosure of the information, or
- If it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

Note: Access to records cannot be refused where this other individual is a Health Professional who has compiled or contributed to the health record or has been involved in the care of the Data Subject, unless serious harm to that health professional's physical or mental health or condition may result from such disclosure.

Once the request has been processed it will be direct to the appropriate Health Care Professional for approval for release.

Lost Records: If it has been identified that the records being requested have been lost then the service must immediately contact the IG Team and complete an incident form. The IG Team will respond to the requestor.

5.8 **Health Care Professional Approval / Sign-Off**

The Data Protection (Subject Access Modification) (Health) Order 2000 sets out the appropriate health professional to be consulted to assist with subject access requests as the following:

- the health professional who is currently, or was most recently, responsible for the clinical care of the data subject in connection with the information which is the subject of the request; or

- where there is more than one such health professional, the health professional who is the most suitable to advise on the information which is the subject of the request, this also applies where a consultant or health professional has left the organisation.

- Where no suitable health professional is available to advise on access then a health professional with the necessary qualifications and experience should advise on matters to which the information requested relates.

For personnel records requests should be reviewed by a Senior Manager within Human Resources.

The Health Care Professional or Senior Manager, who is signing off the release of records, will be required to complete a sign off form, which should be returned to the IG Team, to be placed in the request folder.

5.9 **Timescale**

The organisation should endeavour to respond within 21 days (but no later than one calendar month e.g. 30 days) from receipt of all information e.g. ID check and fee.

Applications must be in writing.

5.10 **Releasing a Request**

Once the request has been completed / agreed by the Health Care Professional, copies of the data and a covering letter will be sent by Recorded Delivery to the Data Subject or their representative, by the IG Team.

5.11 **Supervised Access**

If either the Data Subject has expressed a preference for sight of the records (rather than copies) or the Health Professional has stated that the Data Subject should not receive copies but be given supervised access only, the service will make arrangements for the Data Subject to view the records with an appropriate Health Care Professional in attendance who can explain entries and terminology.

To avoid unnecessary delays, where separate records are held each of the respective services will be responsible for making arrangements for access to the respective records – unless all agree at the outset that the disclosure arrangements will be co-ordinated by one service.

5.12 **Withholding Information**

Withholding information is considered as the "Non–Disclosure (refusing / withholding) of personal information contained within a record"; this can be partially withholding or fully withholding information.

An individual requesting access to their health records may be refused access to parts of the information if an appropriate Clinician deems exposure to that information could lead to distress:

Should any information be found which might need to be withheld because it would:

- Disclose information relating to or provided by a third person who has not consented to that disclosure **unless**:
  - The third party is a health professional who has compiled or contributed to the health records or who has been involved in the care of the patient.
  - The third party, who is not a health professional, gives their consent to the disclosure of that information.
  - It is reasonable to disclose without that third party's consent.

- cause serious harm to the physical or mental health or condition of the Data Subject, or any other person,

Clinicians should be prepared to justify their reasons in a court of law if necessary. In all cases reasons for non-disclosure must be documented in the patient's medical records.

Solent NHS Trust will support any member of staff who, using careful consideration, professional judgement and has sought guidance from their manager, can satisfactorily justify any decision to disclose or withhold information against a patient's wishes. Deliberate, the findings, outcome and decision must be recorded with the patients record.#

Where the third party does not consent, the information may be disclosed providing the identity of the third party is not revealed. The Act suggests that this might be done by omitting names and particulars from the records. Care should be taken to ensure that the

information, if released is genuinely anonymous.

Further guidance should be obtained from the Information Governance Team

The organisation is not required to supply copies of health records if the individual requesting the information has

- not provided enough supporting information in order for the information to be located
- not supplied the necessary evidence of identity

or

- the retrieval of the health records requires disproportionate effort

5.13 **Referring a Request**

If records are not held by the service or organisation then the requestor must be informed and where known the request sent to the appropriate service or Organisation. This will be undertaken by the Information Governance Team.

6 Medical Reports

6.1 Requests for Medical Reports should be forwarded to the relevant Healthcare Professional. Such requests can form part of normal NHS duties and therefore monies received should be credited to the departmental budget. Where medical reports are external to normal NHS duties, and the report has been prepared outside of work hours, monies received will be left to the discretion of the Healthcare Professional.

6.2 The Access to Medical Reports Act 1988 governs access to medical reports made by a medical practitioner who is, or has been responsible for the clinical care of the patient, for insurance or employment purposes. Reports prepared by other medical practitioners, such as those contracted by the employer or insurance company, are not covered by the Act. Reports prepared by such medical practitioners are covered by Data Protection Legislation.

6.3 A person cannot ask a patient's medical practitioner for a medical report on him/her for insurance or employment reasons without the patient's knowledge and consent. Patients have the option of declining to give consent for a report about them to be written.

6.4 The patient can apply for access to the report at any time before it is supplied to the employer/insurer, subject to certain exemptions. The medical practitioner should not supply the report until this access has been given, unless 21 days have passed since the patient has communicated with the doctor about making arrangements to see the report. Access incorporates enabling the patient to attend to view the report or providing the patient with a copy of the report.

6.5 Once the patient has had access to the report, it should not be supplied to the employer/insurer until the patient has given their consent.

7 Third Party Requests

7.1 All third party requests will be processed through the above Subject Access Request process; checks however may vary from request to request.

7.2 Information may be requested from third parties, e.g., solicitors, on behalf of the Data

Subject. Where this is accompanied by authorisation (signed consent) from the Data Subject then this request can be processed using this procedure.

7.3 Where necessary the third party may be contacted for additional details to enable an effective search for the information required for their purpose.

7.4 Where the disclosure request is made by a third party on behalf of a Data Subject who lacks capacity, the Health Care Professional must be consulted and must satisfy him/herself that the disclosure would be in the Data Subject's best interests. If this is not the case, disclosure cannot proceed. The HCP must ensure that justifiable reasons are documented for withholding the disclosure.

7.5 The 'Every Child Matters' (Cross Government Guidance – Sharing Information on Children and Young People), should be followed in conjunction with the guidance given here in this document.

7.6 The 'No Secrets: Guidance on developing and implementing multi-agency policies and procedures to protect vulnerable adults from abuse'. DH 2000 should be followed in conjunction with the guidance given here in this document

7.7 **Subject Access for a Minor**

Parents can make subject access requests on behalf of their children who are too young (under the age of 13) to make their own request. Normally a person with parental responsibility will have the right to apply for access to their child's health record. However, in exercising this right a health professional should give careful consideration to the duty of confidentiality owed to the child before disclosure is given.

Parental Responsibility[1]:

While the law does not define in detail what parental responsibility is, the following list sets out the key roles:

- providing a home for the child
- protecting and maintaining the child
- disciplining the child
- choosing and providing for the child's education
- determining the religion of the child
- agreeing to the child's medical treatment
- naming the child and agreeing to any change of the child's name
- accompanying the child outside the UK and agreeing to the child's emigration, should the issue arise
- being responsible for the child's property
- appointing a guardian for the child, if necessary
- allowing confidential information about the child to be disclosed

A mother automatically has parental responsibility for her child from birth. However, the conditions for fathers gaining parental responsibility varies throughout the UK.

In England and Wales, if the parents of a child are married to each other at the time of the birth, or if they have jointly adopted a child, then they both have parental responsibility. Parents do not lose parental responsibility if they divorce, and this applies to both the resident and the non-resident parent.

[1] http://www.direct.gov.uk/en/parents/parentsrights/dg_4002954

`This is not automatically the case for unmarried parents. According to current law, a mother always has parental responsibility for her child. A father, however, has this responsibility only if he is married to the mother when the child is born or has acquired legal responsibility for his child through one of these routes:

- (from 1 December 2003) by jointly registering the birth of the child with the mother
- by a parental responsibility agreement with the mother
- by a parental responsibility order, made by a court
- by marrying the mother of the child

A father can apply to the court to gain parental responsibility and if awarded proof of parental responsibility will be provided.

For births registered in Scotland and Northern Island refer to
http://www.direct.gov.uk/en/parents/parentsrights/dg_4002954

Access made by a minor: The right of access by a minor should be assessed by application of the same tests as those used in consent to treatment issues. A young person aged 13 or above is generally considered mature enough to understand what a subject access request is. They can make their own request and would need to provide their consent to allow their parents to make the request for them. HCP's must use your judgement to decide whether a young person aged 13 or above is mature enough to make their own request as they do not always have the maturity to do so.

If children are competent to give consent for themselves, consent should be sought directly from them. The legal position regarding 'competence' is different for children aged over and under 16.

Children aged 16 and 17: Once children reach the age of 16, they are presumed in law to be competent to make decisions about their healthcare. This means that in many respects, they should be treated as adults and if they request access to their records at this age, and are considered competent, access should be granted.

Once a child reaches the age of 18 and is deemed competent, no-one else can make decisions on their behalf. Therefore access requests cannot be made by a third party on their behalf.

Children with Learning Disabilities: It should not be assumed that a child with learning disabilities is not competent to make his/her own decisions. Many children will be competent if information is presented in an appropriate way and they are supported through the decision-making process.

7.8 **Requests received for a patient with mental impairment**

The mental Capacity Act 2005 came into force on 01st April 2007. The Act provides a statutory framework to empower and protect people who may lack capacity to make some decisions for themselves, for example those with dementia, learning disabilities, mental health problems, stroke or head injuries who may lack capacity to make certain decisions. The Act will only affect people aged 16 or over.Under common law, there is the presumption that a person seeking to exercise legal rights has the necessary legal capacity to do so. Where the Data Subject is incapable of managing his or her own affairs, a person appointed by a court to manage those affairs might have a right of access to the Data Subject Personal

Data. The specific requirements of the court order or the power of attorney should be considered carefully and followed.

7.9 **Requests by others.**

Any decision to disclose confidential Personal Data outside of Subject Access Requests must be justified on the grounds that there is a court order or statutory provision requiring disclosure or, exceptionally, because the public interest requires it and in any event in compliance with Data Protection Legislation. Access should be restricted to the information necessary.

Such requests should be dealt with in liaison with the Information Governance Team.

Examples of this are (but not limited to) the HMRC, Home Office, etc…

7.10 **Police Requests**

Guidance on dealing with requests from the Police/Court Orders is available within the appendices**.** However, to summarise information should not be released unless the police have provided a Data Protection exemption form (DP2). This form will be reviewed by either the Trust's Date Protection Officer of Assistant Data Protection Officer, to ensure that the exemption is appropriate.

Only copies must be provided, unless a court order is provided for originals, in which case stringent preparation of the records must take place to ensure there completeness.

7.11 **Missing People**

Occasionally the Police will request services to search their records to assist in the search of a missing person. Such requests should also be accompanied by a DP2 form and advice should be sought from the Information Governance Team.

7.12 **Child Protection Request**

If the records/patient are under review by the Child Protection Team, then the Child Protection Team must be contacted prior to the release of records.

Staff are to be supported by the Child Protection Team if they are required to give a statement to the police on a Child Protection matter.

7.13 **Safeguarding Adult Requests**

If the records/patient is under review by the Safeguarding Adults Team, then the Safeguarding Adults Team must be contacted prior to the release of records.

Staff are to be supported by the Safeguarding Adults Team if they are required to give a statement.

7.14 **Requests from Commissioning Organisations**

Requests for medical records maybe received from commissioning organisations, in order to deal with a compliant and/or a litigation claim. These requests should not be handled any differently to any other request.

The commissioning organisation should provide proof of written consent from the client, authorising the commissioning organisation to act on their behalf.

7.15 **Requests from the Department of Work and Pensions**

Health Organisations are required to complete forms from the Department of Work and Pensions. No consent from the patient is required. These types of requests are not considered Subject Access Requests and therefore can be action direct by the relevant HCP.

8 Deceased Patient Records Requests

8.1 Access to the records of a deceased person fall under the Health Records Act 1990

8.2 The Access to Health Records Act 1990 (AHRA) provides a small cohort of people with a statutory right of to apply for access to information contained within a deceased person's health record

8.3 For access to records relating to the deceased, applications may only be received from: -

- ✓ the patient's personal representative (as described in section 8.5), and
- ✓ Any person who may have a claim out of the patient's death.

8.4 However access is NOT to be given to the record or any part of it, if:

- ✓ a note is included in the record, that the patient did not wish access to be given, or
- ✓ the patient had given the information and would not have expected it to be disclosed, or
- ✓ It would disclose information that is not relevant to any claim.
- ✓ disclosure would cause serious harm to the physical or mental health of any other person;
- ✓ would identify a third person, who has not consented to the release of that information.

8.5 A personal representative is the executor or administrator of the deceased person's estate. The personal representative is the only person who has an unqualified right of access to a deceased patient's record and need give no reason for applying for access to a record. Individuals other than the personal representative have a legal right of access under the Act only where they can establish a claim arising from a patient's death. The decision as to whether a claim actually exists lies with the record holder.

8.6 Record holders must satisfy themselves as to the identity of applicants who should provide as much information to identify themselves as possible. Where an application is being made on the basis of a claim arising from the deceased's death, applicants must provide evidence to support their claim. Personal representatives will also need to provide evidence of identity.

8.7 Information will be required to establish a link between the requester and the deceased. A copy of the death certificate and a description as to relationship with the person making the request or valid reason for access should be sought.

8.8 **Process:** The same process is to be followed as that of a Subject Access Request

9 Freedom of Information (FOI) Requests and Environmental Information Regulations (EIR) Requests

9.1 The FOI Act is part of the Government's commitment to greater openness and accountability in the public sector and enables members of the public anywhere in the world to request information held by public authorities. This will further help transform the culture of the public sector to one of greater transparency. The Act is fully retrospective.

9.2 The main features of the FOI Act are;

- A general right of access to recorded information held by public authorities, subject to certain exemptions
- Recorded information includes; agendas, meeting minutes, personal notebooks, emails and CCTV footage. Members of the public can request current or retrospective information
- In cases where information is exempt from disclosure exempt where an absolute exemption applied (e.g. S40 personal information) there is a duty to;
  - Inform the applicant whether the information is held
  - Communicate the information unless the public interest in maintaining the exemption in question outweighs the public interest disclosure
- A duty to maintain a Publication Scheme on the organisations public facing website
- The Information Commissioners Office regulates compliance of the FOI Act and investigates any escalated internal review complaints.

9.3 The EIR gives people the right to see information held by public authorities about the environment, this information may include;

- Land and built structures, when they are affected by environmental factors
- Waste, emissions, noise, energy, radiation (or radioactive waste)
- Air, water, soil, flora and fauna
- The state of human health – collective health as opposed to individual, for example public health issues such as SARS and asbestosis
- Contamination in a food chain, for example BSE

9.4 The main difference with accessing information under EIR is that the request can be in any format, written or verbal (phone/letter or written or email),

9.5 All information requests under FOI and EIR will be processed in accordance with this policy and processed by the IG team.

9.6 **Valid requests:** For a request to be valid under the FOI Act it must be;

- **In writing;** this can be letter or email
- **Include the requestors name;** this could be the name of an organisation, by one person on behalf of another, such as a solicitor or personal representative
- **Include an address for correspondence;** this can be an address at which we can respond to the requestor, including a postal or email address
- **Describe the information requested;** The FOI Act covers information as well as documents, so a requestor does not have to name a specific document. A specific topic may be given and it is expected that relevant information is gathered in order to satisfy the request
- The requestor does not need to state a reason for the request

9.7 There may be occasions when applicant cannot request information in written format. In such cases, assistance should be given either by suggesting a representative makes a request on their behalf, they contact Citizens Advice Bureau or the request handler makes a note of the requested information and sends the paper to the requestor asking for confirmation before the application is processed.

9.8 **Process:** All requests for information are to be forwarded or directed to the Information Governance Team, to ensure that the appropriate steps are undertaken in accordance with

the timeframe standards set out in legislation, please refer to the appendices for full process

9.9 Prior to release of information services must provide all relevant information requested held by the organisation;

- Information the services hold
- Information individuals hold e.g. on personal computer drives
- Emails and other communications (if requested)
- Information held by the Trust, but created by a third party (with their permission)
- If the information is not held in the formal requested, the IG team should be informed
- If the information is not held, it is best practice to advise who or where this information may be held
- Not being able to locate a document does not excuse the organisation from its FOI or EIR obligations.

9.10 **Costs:** There is not normally a charge for FOI/EIR requests for information. However the appropriate limit charge for a request is £450 (£25 standard hourly rate = total 18 hours). The duty to comply with a request for information does not arise if we estimate the cost of compliance with the request would exceed the appropriate limit established in national Fees Regulations. The Trust will work with applicants to keep compliance costs to a minimum but reserves the right to (a) refuse or (b) charge for the communication of information that exceeds the limit. Requestors will be required to pay any fees within a three month period beginning on the day on which the fees notice is issued.

Applicants will be required to pay any fees within a period of three months beginning with the date on which the fees notice is sent from the Trust.

9.11 **Refusing requests:** Requests for information can be refused if;

- It falls under an exemption
- If a request for fee notice has been issued and a fee has not been received within 3 months
- If the cost of providing the information exceeds appropriate limits
- If it can be demonstrated that the request for information is vexatious or repeated

9.12 Where Solent NHS Trust feels an exemption does apply, the IG team will undertake a public interest test, where applicable to decide whether it is more in the public interest to supply the information or whether it is more in the public interest not to supply the information.

9.13 **Transferring requests for information:** If the organisation does not hold all/some of the information requested, but is aware that another Public Authority holds the information, it may transfer the request. The IG team will inform the requestor that the information is not held by Solent NHS Trust, and inform them of the alternative organisation and offer the FOI details for that organisation.

9.14 **Time limits for compliance with requests**

Requests must be responded to with either a disclosure or exemption within 20 working days to meet statutory legal requirements.

The start date of a requests timescale is the next working day after the request is received. A working day is considered Monday – Friday, 9am – 5pm. If a request is received Monday – Friday before 9am the timescale starts from 9am that working day e.g. if a request is received at 8.59am on Monday then the request will be logged and the timescale started

from 9am that Monday, as this is then considered the next working day.

The current guidelines set out by the Information Commissioner aims for Trust's to be compliant to the time limit for the release of requests with at least 95% of requests. Should the Information Commissioner become aware of a consistent failure to respond to requests within the time limit, they may issue an Enforcement Notice. Failure to comply with an Enforcement Notice can be referred to High court and may result in finding of contempt of Court.

10 Publication Scheme

10.1 Solent NHS Trust is mandated to produce a Publication Scheme developed and maintained by the IG team. This is permissible under Section 20 of the FOI Act and ensures compliance with Section 19 of the legislation.

10.2 A Publication Scheme is a proactive approach to making information available. It sets out details of information routinely made available by the Trust, how information can be obtained and any applicable charges. In principle, the more information made publically available within a Publication Scheme, the fewer requests the organisation should receive, unless the request is of a specific nature.

10.3 The Publication Scheme will also be made available in hard copy upon request and can be translated through Access to Communications. It will be subject to regular review in terms of content.

10.4 Applications for information listed within the Trust's Publication scheme may only be received in writing (including email), if the document is not accessible through website and links. The organisation has established systems and procedures to process applications arising from the Publication Scheme.

10.5 The IG team will continuously review, monitor and update the Publication Scheme.

11 Complaints Process

11.1 If a requestor is dissatisfied with the handling of any of the requests for information covered by this policy, they have the right to ask for an internal review. Internal review requests should be submitted within two months of the date of receipt of their response letter and should be addressed to: Data Protection Officer, Solent NHS Trust, Highpoint Venue, Southampton, SO19 8BR or InformationGovernanceTeam@solent.nhs.uk

12 Roles and Responsibilities

12.1 Chief Executive

The Chief Executive as the Accountable Officer has overall responsibility for compliance with legislation within the Organisation. An accountable officer is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

The Chief Executive has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

12.2 **Caldicott Guardian and Senior Information Risk Officers (SIRO)**

The Organisation's Caldicott Guardian and SIRO have a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

12.3 **Information Asset Owners**

The Information Asset Owner (IAO) is a senior member of staff who is the owner for one or more identified information assets of the organisation.

It is the responsibility of the IAO to ensure that all FOI requests received by them, from the Information Governance Team, are cascaded appropriately and dealt within in timely manner in accordance with the Act.

12.4 **Information Governance Team**

The Information Governance Team is responsible for the overall development and maintenance of all requests for information practices throughout the organisation, in particular for co-ordinating all requests and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of patient information. The Information Governance Team will ensure all FOI responses are approved appropriately. Complex responses will be authorised by the SIRO and Director of Strategy prior to disclosure.

The IG Team are required to maintain expert knowledge in all legislation pertaining to requests for information, covered by this policy. They must also ensure that they review all responses / releases to ensure only appropriate information is released and it is only released to those who are legally entitled to it.

12.5 **Information Asset Custodians**

Information Asset Custodians are responsible for assisting in the co-ordination of all requests in the execution of their duties, offering advice and training to all staff who are likely to deal with such requests. Information Asset Custodians are also responsible for ensuring up-to-date documents are available on the publication scheme.

12.6 **Health Care Professionals**

Healthcare professionals are responsible for assessing and review the clinical records that they have contributed to, prior to the records being released.

All users of Healthcare Records must be aware of their legal obligations and abide by the requirements of the Data Protection Act and Principles of Caldicott.[2]

All users of Healthcare Records must be aware of the process for managing Freedom of Information requests and act on it as required.

12.7 **All Staff**

All staff are obliged to be aware of the FOI Act and Data Protection Legislation, and co-operate with requests for information in accordance with this policy. A failure to adhere to this Policy and its associated procedures may result in disciplinary action. Managers at all levels are responsible for ensuring that the staff for whom they are responsible are aware of and adhere to this Policy. They are also responsible for ensuring staff are updated in regard

[2] NHSLA RM Evidence Template

to any changes in this Policy.

13 Training

13.1 All Trust staff will be made aware of their responsibilities regards Data Protection and FOI, through their annual Information Governance Training.

13.2 It is the responsibility of the Information Governance Team to produce the training tool

13.3 Compliance with this training requirement will be monitored by the Learning & Development Team in conjunction with the Information Governance Team via a reporting mechanism learning and development training tool.

14 Equality Impact Assessment and Mental Capacity

14.1 A thorough and systematic assessment of this policy has been undertaken in accordance with the Trust's Policy on Equality and Human Rights.

14.2 The assessment found that the implementation of and compliance with this policy has no impact on any Trust employee on the grounds of age, disability, gender, race, faith, or sexual orientation. See Appendix A

15 Success Criteria / Monitoring Effectiveness

Data Security & Protection Toolkit:
The monitoring of this policy and its effectiveness and maintenance will be audited annually using the DSPT or sooner if new legislation, codes of practice or national standards are introduced. The DSPT it is a self assessment audit undertaken by the Information Governance Team. In addition to this the DSPT is audited annually by the Trust's Internal Auditors.

The owner/author of the policy is responsible for undertaking this audit and ensuring the policy's effectiveness.

The implementation of this policy will be audited annually by the Information Governance Team who will also perform spot check audits to assess compliance.

The Information Governance Team will on a weekly basis review and monitor all Information Requests

16 Non-compliance

Failure by any employee of Solent NHS Trust to adhere to the policy and its guidelines will be viewed as a serious matter and may result in disciplinary action.

Where employees believe that it is not possible to uphold the policy and associated guidelines they must bring this to the attention of the Data Protection Officer and Head of Information Governance & Security

17 Review

This document may be reviewed at any time at the request of either staff side or management, but will automatically be reviewed 3 years from initial approval and thereafter on a triennial basis unless organisational changes, legislation, guidance or non-compliance prompt an earlier review.

Appendix A: Equality Impact Assessment

Step 1 – Scoping; identify the policies aims	**Answer**		
1. What are the main aims and objectives of the document?	To outline the Trust's legal responsibilities for complying with requests for information held by the Trust		
2. Who will be affected by it?	Patient information, Staff information, all services / staff		
3. What are the existing performance indicators/measures for this? What are the outcomes you want to achieve?	There is a minimum requirement set by the Information Commissioner's Officer to maintain a 95% compliance rate with all requests for information		
4. What information do you already have on the equality impact of this document?	None expected		
5. Are there demographic changes or trends locally to be considered?	No		
6. What other information do you need?	N/A		
Step 2 - Assessing the Impact; consider the data and research	**Yes**	**No**	**Answer** (Evidence)
1. Could the document unlawfully discriminate against any group?		X	
2. Can any group benefit or be excluded?		X	
3. Can any group be denied fair & equal access to or treatment as a result of this document?		X	
4. Can this actively promote good relations with and between different groups?	X		
5. Have you carried out any consultation internally/externally with relevant individual groups?		X	Legal requirements
6. Have you used a variety of different methods of consultation/involvement	X		
Mental Capacity Act implications			
7. Will this document require a decision to be made by or about a service user? (Refer to the Mental Capacity Act document for further information)		X	
External considerations			
8. What external factors have been considered in the development of this policy?	X		Legislation
9. Are there any external implications in relation to this policy?	X		Legislation
10. Which external groups may be affected positively or adversely as a consequence of this policy being implemented?			All positively, open access to information, within legal perimeters

Appendix B: Subject Access Request Process
Appendix C: Health Care Professional Guidance
Appendix D: FOI Process
The above can be found
http://intranet.solent.nhs.uk/TeamCentre/InformationGovernance/Pages/InformationRequests.aspx