National Data Opt-out Policy

|  |  |
| --- | --- |
| Version number : | 1.0 |
| Consultation Groups | Information Governance Steering Group |
| Approved by (Sponsor Group) | Information Governance Steering Group |
| Ratified by: | Quality Committee |
| Date ratified: | June 2022 |
| Name of originator/author: | Associate Director for Business Intelligence and Analytics |
| Executive Director lead : | Chief Quality Officer |
| Implementation Date : | June 2022 |
| Last Review Date | June 2022 |
| Next Review date: | March 2025 |

|  |  |
| --- | --- |
| Services | Applicable |
| Trustwide | All Staff |
| Mental Health and LD |  |
| Community Health Services |  |

Version Control Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Status** | **Comment** |
| Draft | March 2022 | Associate Director of Business Intelligence and Analytics | Draft | Circulated for consultation prior to submission at November April IGSG |
|  |  |  |  |  |

Contents

| **Paragraph** | | **Page** |
| --- | --- | --- |
| 1 | Introduction | 4 |
| 2 | Purpose | 4 |
| 3 | Duties and Responsibilities | 4 |
| 4 | Process | 6 |
| 5 | Information for Patients | 7 |
| 6 | Data protection and privacy impact assessments | 7 |
| 7 | Training | 8 |
| 8 | Trust Compliance with this policy | 8 |
| 9 | Staff Compliance with this policy | 8 |
| 10 | Information governance incidents | 9 |
| 11 | Monitoring, amendments and document control | 9 |
| 12 | Legal Considerations | 9 |
| 13 | References | 10 |

1. **Introduction**

In response to the National Data Guardian (NDG) review of data security and how health care organisations use and share data, the National Data Opt-out Programme (NDOP) was developed. NDOP will allow patients registered in England to control how their data is shared for secondary purposes, further from the initial purpose for which data were collected.

This policy is underpinned to ensure that proper data security, management and technical measures exist and are embedded throughout the Trust.

The Trust is committed to treating people with dignity and respect in accordance with the Equality Act 2010 and Human Rights Act 1998. Throughout the production of this policy due regard has been given to the elimination of unlawful discrimination, harassment and victimisation (as cited in the Equality Act 2010).

1. **Purpose**

The purpose of this policy is to provide a consistent and logical framework to ensure that the patient's opt-out choice is respected at the Trust.

This policy applies to all Staff handling information at the Trust including contractors, locums, students and volunteers. All technologies, hardware, software and peripheral equipment owned and provided by the Trust. All Information and data the Trust holds in any format. All new and developing technologies, which may not be explicitly referred to.

1. **Duties and Responsibilities**

**3.1 The Chief Executive (CE)** has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level.

The responsibility to ensure proper data security is delegated through the Trust management structure, with specific responsibilities allocated as below:

**3.2 The Senior Information Risk Owner (SIRO)** acts as the advocate for information risk on the Board and oversees any risks related to clinical data. The SIRO is responsible for owning, supporting and adhering to this policy.

**3.3. The Caldicott Guardian** acts to ensure that procedures are in place to govern access to and the use of personal identifiable and confidential information. Provide leadership and informed guidance on complex matters involving confidentiality and information sharing. Oversee all arrangements, protocols and procedures where confidential personal information may be shared with external bodies

**3.4 The Associate Director of Information Governance / Data Protection Officer** ensures that person identifiable data is processed according to data protection law and best practice.

**3.5 All managers** are required to ensure compliance with this policy and that the staff for whom they are responsible are aware of and adhere to this policy.

**3.6 All staff**

To seek advice from the Information Governance team on whether the National Data Opt-out applies to their data activities and how it can be implemented in their area.

Every member of staff is responsible for taking precautions to ensure the security of information, both whilst it is in their possession and when it is being transferred from one person or organisation to another. If staff are unsure about sharing information, they should refer to the Data Protection and Confidentiality Policy, Data Protection and Privacy Impact Assessment Policy, Information Governance Policy, Information Governance Strategy, the NHS Confidentiality Code of Practice, or take advice from their line manager, the Information Governance Department or the Caldicott Guardian, as appropriate.

Be aware of information risk management and understand the need for information risk to be a part of the trust culture.

Are familiar with the data protection principles, Caldicott Guardian principles and documented procedures within this policy.

Carry out day-to-day work in accordance with best practice confidentiality and data protection procedures and legislation.

Keep up to date with best practice confidentiality and data protection procedures and legislation through undertaking annual Information Governance training.

Understand and adhere to, the Privacy and Data Protection Legislation and other legal requirements including the Confidentiality NHS Code of Practice to support the Caldicott Guardian and safeguard against harm to individuals or the trust’s

**3.7 Information asset owners**

Understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result, they can identify, understand and address risks to the information assets they 'own'.

Ensure that risk assessments are undertaken on all information assets.

Assure the Senior Information Risk Owner on the security and use of the information assets

**3.8 Clinical Systems Managers**

Ensure organisational, technical and security measures exist to the system they manage. This may include implementing standard operating procedures for the use and management of the system to help the Trust to ensure higher levels of security over the information processed within the system

**3.9 Informatics (Business Intelligence, Analytics and Data Warehouse Team)**

Owning and maintaining process to identify patients who have chosen to be included in the National Data Opt-out, minimising the unnecessary processing of patient data for purposes beyond direct care.

Identifying patients who have chosen to be included in the National Data Opt-out.

1. **Process**

**4.1 National Opt Out Assessment**

Before sending data outside the trust staff must conduct an assessment as to whether national data opt out applies.

It applies if the following 2 conditions are true

**When the data contains patient confidential or sensitive data**

*(This is when two types of patient information are joined together. The two types of information are a person's identity and information about his or her health care or treatment, for example, their name along with the treatment they received or their NHS number along with the medication given)*

**AND**

**The data is not anonymised before disclosing.**

(This is when the data from which the patient cannot be identified by the recipient of the information)

**4.2 National Opt Out Check via MESH – NHS Digitals central repository for national data opt-outs**

NHS Digital has developed a technical service known as MESH, which enables the Trust to check if patients have a national data opt-out to respect the patient's opt-out choice at the Trust.

The Trust can submit a list of NHS numbers that they need to disclose and the MESH service looks these up against the central repository of national data opt-outs. To support the data transfer via MESH, a file must be sent containing just the NHS Numbers in a single column of a excel spreadsheet.

The MESH service returns a “cleaned list” of those that do not have a national data opt-out i.e. it removes the NHS numbers for those with a national data opt-out.

To carry out this check please provide the excel file with NHS numbers to the Informatics team who will contact the MESH elt-tr.Performance@nhs.net

The informatics team will then return the list of valid NHS numbers. The trust staff must then remove any patients from their data that does not have a NHS number contained in the file retuned from Informatics via the MESH.

1. **Information for Patients**

Patients can set or change their national data opt-out choice using an online or contact centre service. When a patient sets a national data opt-out it is in held in a repository on the NHS Spine against the patient’s NHS number. National data opt-outs may take up to 21 days from being registered with NHS Digital to being fully applied to all disclosures of data.

Patients can view or change their national data opt-out choice at any time by using the online service at **[www.nhs.uk/your-nhs-data-matters](http://www.nhs.uk/your-nhs-data-matters)**.

Or by clicking on "Your Health" in the NHS App, and selecting "Choose if data from your health records is shared for research and planning".

Staff can use the 'Your Data Matters to the NHS' resources at **<https://digital.nhs.uk/services/national-data-opt-out/supporting-patients-information-and-resources>** to help raise awareness.

1. **Data protection and privacy impact assessments**

Risks to personal, confidential or sensitive information that arise as a result of the following activities must be further assessed and documented through the completion of data protection and privacy impact assessment (DPIA).

* The use of a trial period of technology, modalities or products, which use data or information.
* The use of charitable or free technology, modalities or products, which use data or information.
* Publishing personal identifiable or sensitive information or data on the internet or in other publicly available media types.
* Procurement of technology, modalities or products, which use data or information.
* De-commissioning or disposal of technology, modalities or products, which use data or information
* A change to existing processes or technology, modalities and products, which will significantly amend the way data or information, is handled.
* The implementation or development of new processes, technology, modalities or products, which involve the use of data or information.
* Collection, retrieval, obtaining, recording or holding of new data or information.

The DPIA should be completed by any member of staff who is a person responsible for accomplishing the project objectives and outcomes.

The Data Protection by Design Policy sets out the basic steps which all staff should understand and must follow during the initiation phase or early assessment for the development, implementation of projects at the trust.

The DPIA processes and templates are available from the information governance team at [elft.information.governance@nhs.net](mailto:elft.information.governance@nhs.net)

1. **Training**

The Data Security Awareness Level one course is mandated for everyone working in health and care. It has been designed to inform, educate and upskill staff in data protection, data security and information sharing. It provides an understanding of the principles and importance of data security and information governance. It looks at staff responsibilities when sharing information and includes a section on how to take action to reduce the risk of breaches and incident

For additional learning support, staff should contact [elft.information.governance@nhs.net](mailto:elft.information.governance@nhs.net)

1. **Trust compliance with this policy**

Article 5(1) of the UK GDPR states that personal data shall be (a) processed lawfully, fairly and in a transparent manner in relation to the data subject. Therefore, the trust has a legal obligation to:

* Identify a ‘lawful basis’ for collecting and using personal data.
* Ensure data is processed in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.
* Ensure that the trust tells people about data processing to be open and honest before their data is used.

1. **Staff compliance with this policy**

Any breach of, or refusal to comply with this policy may lead to action in accordance with relevant trust policies and procedures. In serious cases, a breach may be regarded as gross misconduct and may result in dismissal.

Individuals may be personally charged under criminal or civil law, and prosecuted for breaches of confidentiality, which are caused by malice or negligence.

Section 170(1) of the Data Protection Act 2018 states that it is an offence for a person knowingly or recklessly:

### To obtain or disclose personal data without the consent of the controller

### To procure the disclosure of personal data to another person without the consent of the controller, or

### After obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained

1. **Information governance incidents**

It is essential that all information governance, incidents are reported on Datix, the Trust’s incident reporting system. The Incident Management Policy and Procedure sets out how to report incidents and near misses.

Everyone is responsible for reporting information incidents such as information being illegitimately accessed, used, disclosed, altered, destroyed, and or stolen, resulting in impairment or loss as soon as possible directly through Datix (no later than the next working day - check).

1. **Monitoring, amendments and document control**

This policy is reviewed on a triennial basis as a minimum or more frequently, as required by NHS England, DoH, NHS Digital and the ICO, to ensure the sections still comply with the current legal requirements and professional best practice, to provide value to the policy.

1. **Legal considerations**

The trust regards all identifiable personal information relating to patients as confidential and will undertake or commission annual assessments and audits of its compliance with legal requirements. The Trust regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

The trust has established and will maintain policies to ensure compliance with the NIS Regulations 2018, Privacy and Data Protection legislation, the Common Law Duty of Confidence and the Confidentiality NHS Code of Practice.

The trust has established and will maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation.

Failure to comply with the data protection regulations could result in reputational damage to the Trust and may carry financial penalties imposed by the ICO, or other regulatory action.

Under the Network and Information Systems Regulations 2018 (NIS Regulations) and GDPR, there are two tiers of administrative fine that can be imposed:

* The maximum fine for the first tier is €10,000,000 or in the case of an undertaking up to 2% of total annual global turnover (not profit) of the preceding financial year, whichever is greater.
* The second tier maximum is €20,000,000 or in the case of an undertaking up to 4% of total annual global turnover (not profit) for the preceding financial year whichever is greater.
* The fines within each tier relate to specific articles within the Regulation that the organisation has breached.
* As a general rule, organisations who fail to comply with GDPR principles will result in a fine within tier one, while data breaches of an individual’s privacy, rights and freedoms will result in a fine within tier two.

Where the law is unclear, a standard may be set, as a matter of policy, which clearly satisfies the legal requirement and may exceed some interpretations of the law.

**13. References**

## Legislation specific to the subject of this document:

The General Data Protection Regulation 2018

The UK General Data Protection Regulation (after 1 January 2020)

The Data Protection Act 2018

The Common Law Duty of Confidentiality

The Computer Misuse Act 1990

The Freedom of Information Act 2000

The Human Rights Act 1998

The NHS Confidentiality Code of Practice 2003

The NHS Act 2006: Section 251

The Health and Social Care Act 2012: Section 259

## Regulations specific to the subject of this document

Caldicott 2 Review: to Share or Not to Share

Data Sharing Code of Practice