Information Governance

National Opt Out Policy

Policy Reference: OHCPWHN/IG/NOOP V1

Policy Title	National Opt Out Policy	
Author/Contact	Holly Hellstrom – Information Assurance Director	
Document Ref	OHCPWHN/IG/NOOP	
Version	1	
Status	Approved	
Publication Date	September 2023	
Review Date	August 2026	
Approved by	Dr James Britton – Caldicott Guardian Jeremy Fowler – SIRO	27th September 2023
Ratified by	Information Governance Team	27th September 2023

Version	Date	Comments	Author	Notes
1	27/9/2023	Approved by IGT	Information Assurance Director	

Contents

Introduction

Ozone Health Ltd is the overarching board and governance for Ozone Health Ltd (OHL) Clinical Partnership (CP) & The World Healthnet Ltd (WHN).
This policy applies to all companies within the group and hereafter referred to as 'group' or 'organisation'.

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 Organisation.

The Group 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).

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

Definitions

Term	Definition
National Data Opt-Out	Means the mechanism which allows a person to exercise their right to decide whether to allow their personal confidential information to be used for purposes beyond their direct care.
Confidential Patient Information	Means the data that the NDOO applies to. Confidential Patient Information is information which identifies or is likely to identifyan individual, and the individual is owed an obligation of confidence and conveys some information about the physical ormental health or condition of an individual; their diagnosis, and/or their treatment.

Acronyms

Acronym	Term
NDOO	National Data Opt-Out
MESH	Message Exchange for Social Care and Health
PDS	Personal Demographics Service

Duties & Responsibilities

The Information Governance team is responsible for this policy and that regular reviews and updates are undertaken as appropriate.

The Data Protection Officer is responsible for ensuring that this policy meets our legal obligations of data protection and confidentiality.

The Information Assurance Director is responsible for implementing the processes contained within this policy as part of their obligation to process patient data within our health and social care contracts.

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.

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.

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

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.

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, or take advice from their line manager, the Information Governance Team or the Caldicott Guardian, as appropriate.

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.

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.

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 Organisation to ensure higher levels of security over the information processed within the system.

Process

National Opt Out Assessment

Before sending data outside the Organisation 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)

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 Group to check if patients have a national data opt-out, to respect the patient's opt-out choice at the Group.

The Group 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 Information Governance team who will contact the MESH NHS Spine portal.
The team will then return the list of valid NHS numbers. The Information Governance staff must then mark any patients from their data that has chosen to opt out for future data assessments (see Appendix A).

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, 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.

A child may opt-out from the age of 13. Children under 13 or who lack capacity are not able to set an opt-out themselves. In these cases, those who have a legal relationship with theperson may set their opt-out on their behalf by proxy.

Exceptions (out of scope for NDOO)

There can be on occasion a time when NDOO does not apply. This list is not exhaustive:

Explicit consent: Where we have gained explicit consent for a specific purpose from individuals NDOO will not apply.

Communicable diseases: Where the data relates to communicable diseases and is for the purpose of monitoring or control of disease and risk to public health NDOO will not apply.

Overriding public interest: Where we as Data Controllers have assessed the data, as part of an overriding public interest test, to be disclosed in the public interest NDOO will not apply.

Other Legal requirement: Where there is a legal requirement to disclose the information NDOO will not apply. We will assess any legal requirement aside the common law duty of confidentiality in such cases.

Invoice validation: Where CPI data is used for invoicing or payment NDOO will not apply. All efforts will be made to ensure non-identifiable data is used where it is possible.

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.
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.

Training

The Group provide a robust annual Governance Training program. 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.

Group 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 Group 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 Group tells people about data processing to be open and honest before their data is used.

Staff compliance with this policy

Any breach of, or refusal to comply with this policy may lead to action in accordance with relevant Group 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

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.

Legal considerations

The Group 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 Group regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

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

The Group 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 Group and may carry financial penalties imposed by the ICO, or other regulatory action.

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.

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
Regulations specific to the subject of this document:
Caldicott 2 Review: to Share or Not to Share
Data Sharing Code of Practice

Q	Assessment Criteria	Action
1	Is the use or disclosure confidential patient information?	Yes = Go to Q2 No = Not Applicable to NDOO
2	Is the use of disclosure for individual care or research and planning?	Individual Care = Not Applicable Research & Planning = Go to Q3
3	Do you have explicit consent for the use or disclosure?	Yes = Not Applicable to NDOO No = Go to Q4
4	Is the disclosure for the purpose of monitoring and control of communicable disease or other risks to public health?	Yes = Not Applicable to NDOO No = Go to Q5
5	Is the use or disclosure in the overriding public interest?	Yes = Not Applicable to NDOO No = Go to Q6
6	Is the information being disclosed because of a legal requirement?	Yes = Not Applicable to NDOO No = Go to Q7
7	Is the use or disclosure to a national or arms-length body?	Yes = Check the Policy to see exemptions No = Go to Q8
8	Is the use or disclosure to support payment and invoice validation?	Yes = Check that it has to be CPI, if not then anonymise, if so Not Applicable to NDOO No = Go to Q9
9	Is the legal basis for the use or disclosure Section 251 approval?	Yes = Subject to NDOO unless CAG determine otherwise No = Subject to NDOO