

Patient Objection to the Creation or Use of their Health Record Procedure

Document Reference	Proc456
Version Number	2.2
Author/Lead Job Title	Karen Robinson Information Governance Officer
Lead Director name	Hilary Gledhill, Director of Nursing
Consultation	IG Group
Date of Last Changes (This Version)	24 January 2024
Date of Next Review	January 2027
Name of approving Group/Committee/Director Date of approval	Information Governance Group 24 January 2024

VALIDITY – Procedures should be accessed via the Trust intranet to ensure the current version is used.

CHANGE RECORD

Version	Date	Change details
1.0	February 2017	Policy updated to a procedure as agreed at IG Committee November 2016. Policy and system references updated.
1.1	18/09/2018	Updated references to Data Protection Act 2018 and GDPR.
2.0	March 2020	The procedure has been reviewed and updated to include patient objections to being included in the Yorkshire and Humber Care Record and a process for complying with the National Data Opt-Out.
2.1	July 2022	Section 3.6 updated with the functionality for GP practices to apply the opt out and for recipients of data to be notified how many records have been removed. Approved at IG Group (13 July 2022)
2.2	January 2024	Section 3.2 updated to include Type 1 opt outs for research and planning for Trust GP practices. Section 3.5 updated as overall opt out to the YHCR are managed centrally. Local opt out form removed in Appendix 3. Information added in relation to objections recorded in Lorenzo and SystemOne. Removal of the requirement that an objection in one system will be applied to all as different preferences may be selected at different S1 units. References updated. Approved at IG Group (25 January 2024).

Contents

1. INTRODUCTION	3
2. SCOPE	3
3. PROCEDURES	3
3.1. Patient objects to being recorded on a Trust electronic patient record system	3
3.2. Patient wishes to restrict how information is used	4
3.3. Patients who object to a particular disclosure of their information	4
3.4. System-specific Privacy Options	4
3.5. Yorkshire and Humber Care Record (YHCR).....	4
3.6. National Data Opt-Out	5
4. IMPLEMENTATION	6
5. MONITORING AND AUDIT	6
6. REFERENCES/EVIDENCE/GLOSSARY/DEFINITIONS.....	7
7. RELEVANT POLICIES/PROCEDURES/PROTOCOLS/GUIDELINES	7
Appendix 1: Trust Electronic Patient Record Systems	8
Appendix 2: Patient Restriction on the Use of their Personal Information.....	9
Appendix 3 – Flow chart to assess current and ongoing data disclosures.....	10

1. INTRODUCTION

On occasion, a member of staff or a close family member may need to become a user of our services and may object to their information being recorded on any of the electronic record systems in use across the organisation. Please see Appendix 1 for the list of electronic patient record systems currently in use within the Trust.

Patients are entitled to object to information they provide in confidence being disclosed to a third party in a form that identifies them, even if this is someone who might provide essential healthcare. Patients may also place restrictions on how their personal data is used.

The aim of this procedure is to specify how such objections should be handled in order that patient choice about their information is respected whilst ensuring that information necessary for providing care is available to those who need it.

2. SCOPE

This procedure applies to all patients who raise an objection to their information being recorded on a Trust electronic patient record system or wish to restrict how their personal information is used by the Trust.

3. PROCEDURES

All employees are responsible for maintaining the confidentiality of information gained during their employment by the Trust in line with the Confidentiality Code of Conduct.

All patients will be treated the same way, particularly with regard to confidentiality and robust information governance arrangements are in place to protect personal data.

Records created for the direct care of the individual, whether manual or computer based, will not be anonymised in any way as to conceal the true identity of the patient. When names are anonymised it makes finding patient records virtually impossible, which can have serious implications for the care provided if these records are required urgently, or perhaps outside of office hours. In addition, it also causes difficulty during auditing and issues arise with data quality. For the same reasons, it is not possible for information about patients of the Trust to be recorded in manual form alone.

In addition to enabling safe clinical care, it is essential that records are accessible for medico-legal issues, such as defending the Trust and its employees in matters of clinical negligence.

If privacy or confidentiality concerns are raised by the patient or manager, an audit trail can be produced following the Information Governance IT Forensic Investigations and Confidentiality Audit Procedure.

A patient is entitled to restrict how the Trust's uses their personal information and who the Trust shares that personal data with. The Trust will respect such a restriction unless there are exceptional circumstances, see Confidentiality Code of Conduct (Section 9.9) for further information.

3.1. Patient objects to being recorded on a Trust electronic patient record system

If a patient raises concerns about being recorded on a Trust system, the patient should be:

- reassured about the confidentiality and security of Trust systems
- advised about the availability of the audit trails for Trust systems
- advised about any system restrictions that are available to them

Ultimately, if a patient is unable to engage in treatment due to complicating factors such as not consenting to a Trust medical record in line with Trust system and requirements, the primary care or secondary service provider should seek funding from the local commissioner to access care elsewhere.

3.2. Patient wishes to restrict how information is used

The Trust advises all patients about how their information is used using a patient privacy notice. If a patient objects to their information being used for purposes other than their care, they are advised to speak to their key worker. Objections must be put in writing and the form in Appendix 2 may be used for such purposes.

A copy of the letter/form must be forwarded to the Medical Records Administration Manager who will mark the appropriate systems with the restriction. The key worker must ensure that the original letter/form is scanned into the electronic health record.

Most patients do not place such restrictions. However, any processing of their data for purposes other than direct healthcare must still comply with the Data Protection Act 2018, General Data Protection Regulation (GDPR) and other information governance rules.

Patients at Trust GP practices can stop the practice from sharing their data for research and planning purpose by registering a Type 1 Opt-Out using [this form](#). The GP practice will add the necessary SNOMED code and scan a copy of the form to the electronic record.

3.3. Patients who object to a particular disclosure of their information

Patients do have the right to object to information they provide in confidence being disclosed to a third party in a form that identifies them, even if this is someone who might provide essential healthcare (subject to certain exemptions detailed in the Confidentiality Code of Conduct – Section 9.9). They may also limit the consent given. Where patients are competent to make such a choice and where the consequences of the choice have been fully explained, the decision should be respected. This is no different from a patient exercising his or her right to refuse treatment.

In such circumstances staff should:

- Clearly establish the concerns of the patient and look at whether there is a technical or procedural way of satisfying the consent without unduly compromising care.
- Explore the options for providing an alternative form of care or to provide care through alternative arrangements.
- Assess the options that might be offered to the patient, balancing the risks, staff time and other costs attached to each alternative that might be offered against the risk to the patient of not providing healthcare.

Careful documentation of the decision-making process and the choices made by the patient must be included within the patient's record or the explicit consent form that will be included in the patient's record.

3.4. System-specific Privacy Options

Some systems have specific privacy options available to patients. For example, SystmOne allows patients to mark entries as private and also requires patient consent for the sharing of the record. Details about these privacy options are covered in the [SystmOne Enhanced Data Sharing Module SOP](#) (eDSM).

3.5. Yorkshire and Humber Care Record (YHCR)

The Trust participates in the Yorkshire and Humber Care Record (YHCR) and will make available information from our clinical systems to others providing health and social care to the patient. Patient data will be accessed on a permission to view basis.

Patients with an objection to the sharing of information for direct care purposes in Lorenzo will not be included in the YHCR project. A consent flag will be included in the Upstream system.

Patients can object to the sharing of information with the YHCR by contacting hnf-tr.yhcr@nhs.net. This is to opt out of all YHCR sharing and relevant data controllers will be notified.

The IG Team will confirm with the health professional whether there is any reason not to uphold the objection. Any decision not to uphold the patient's objection must be approved by the Caldicott Guardian. The IG Team will ensure that all objections are recorded in the primary system for the patient.

It is not currently possible to restrict individual documents from sharing with the YHCR. The health professional must make this clear to the patient if they ask for specific information to be excluded from sharing with the YHCR. Patients who do not want specific information to be shared will need to opt-out of the YHCR.

Information shared with the YHCR directly from SystmOne will apply the patient's information sharing consent registered in the unit and will not share records with a dissent recorded. Any entries marked private in the unit will not be shared with the YHCR.

3.6. National Data Opt-Out

The National Data Opt-Out allows patients to opt-out of their personal confidential data being used research and planning purposes. It applies across the health and adult social care system in England.

Patient can opt out online, via the NHS App, by telephone or by paper form. The opt-out is stored against the person's NHS number on the NHS Digital Spine.

The Trust Privacy notice includes the recommended NHS Digital's Template Transparency Statement.

When the opt-out applies

The opt-out applies to confidential patient data shared for research or planning purposes where Section 251 NHS Act 2006 approval has been granted by the Confidentiality Advisory Group (CAG) as the lawful basis for sharing information under the Common Law Duty of Confidentiality. In some cases, the CAG may advise that the National Data Opt-Out does not apply and this will be specified in the CAG Approval Letter.

The opt-out applies regardless of the format of the data and this includes structured and unstructured electronic data and paper records. When the opt-out is applied, the entire record (or records) associated with that individual must be fully removed from the data being disclosed.

When the opt-out does not apply

- Information shared for direct care
- Legal requirements to share information e.g. court order
- Information shared on a case by case basis in the public interest
- Information shared with the explicit consent of the patient
- Anonymised data in line with the Information Commissioner's Code of Practice on Anonymisation or aggregate or count type data.
- When there is an exemption, examples given in NHS Digital: [data-opt-out-data-uses-release-compendium](#)

Identifying data flows within the Trust

It is essential that all new disclosure requests for purposes beyond direct care are assessed to consider whether the national data opt-out policy applies. The flow chart in Appendix 3, will be followed to identify data disclosures which are in scope.

Information Asset Owners (IAO) will ensure that their Records of Processing Activities (ROPA) are kept up to date with the data flows, ensuring that data flows reliant on Section 251 NHS Act 2006 are identified. The IAO will provide updated ROPA to the IG Team with any new disclosures.

The Information Governance Team will review all ROPA to ensure that data flows in scope are recorded accurately. The IG Team will obtain a copy of the Section 251 Approval summary for the data flow from the Health Research Authority CAG registers (<https://www.hra.nhs.uk/planning-and-improving-research/application-summaries/confidentiality-advisory-group-registers/>). For data flows that are not subject to the opt-out, the IG Team will obtain a copy of the CAG approval letter.

The IG Team will report to the IG Group on a quarterly basis, data flows that fall within the scope as part of the standing agenda item for Record of Processing Activities.

Applying the National Data Opt-Out

Requests for data to be checked against the national data opt out should be submitted to hnf-tr.bi-hub@nhs.net. Business Intelligence Team will use the Message Exchange for Social Care and Health (MESH) to send a list of NHS number to be checked against the repository on the Spine. Business Intelligence will receive the list back, with the NHS number removed of any patients that have a national data opt-out. The [NHS Digital: Check for National Data Opt-Outs Service](#) guidance will be followed.

Business Intelligence or the Team disclosing the information will remove the entire records of those patients who have opted out from the data flow. The data will not be removed from the patient's original care record. A record of the disclosure will be retained for the length of time specified within the Records of Processing Activity.

For GP Practices this functionality has been added to Clinical Reporting tree within SystemOne. For any flows that apply, under Data Dissemination, Practices should tick "Apply National Data Out-Out Preferences". All reports that are marked as data disseminations will appear in the Data Dissemination Report Audit when they have been run.

The Team responsible for disclosing the data will notify the receiving organisation that the National Data Opt-Out has been applied and the number of records that have been removed, even if the number is 0.

4. IMPLEMENTATION

This procedure will be disseminated by the method described in the Policy for the Production, Approval and Review of Policies.

5. MONITORING AND AUDIT

Restrictions placed by patients will be monitored to ensure these are appropriately marked on the relevant electronic system.

Data flows with the scope of the National Data Opt-Out will be reported to the IG Group as part of the standing agenda item on the Records of Processing Activities.

6. REFERENCES/EVIDENCE/GLOSSARY/DEFINITIONS

- NHS Digital: National Data Opt-Out Operational Policy - <https://digital.nhs.uk/services/national-data-opt-out-programme/operational-policy-guidance-document>
- NHS Digital: Compliance Implementation Guide - <https://digital.nhs.uk/services/national-data-opt-out-programme/compliance-with-the-national-data-opt-out/compliance-implementation-guide>
- NHS Digital Information Standard DCB3058 Compliance with National Data Opt-Outs - <https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb3058-compliance-with-national-data-opt-outs>
- NHS Digital: Understanding the National Data Opt-Out - <https://digital.nhs.uk/services/national-data-opt-out/understanding-the-national-data-opt-out>
- NHS England: Local Health and Care Records: Information Governance Framework for Integrated Health and Care. [Information Governance Framework for Integrated Health and Care: Shared Care Records - NHS Transformation Directorate \(england.nhs.uk\)](https://www.england.nhs.uk/infogovernance/framework-for-integrated-health-and-care-shared-care-records/)

7. RELEVANT POLICIES/PROCEDURES/PROTOCOLS/GUIDELINES

SystemOne Enhanced Data Sharing Module (eDSM) SOP

Confidentiality Code of Conduct P162

Information Governance and IT Forensic Investigation and Confidentiality Audit Procedures.

Appendix 1: Trust Electronic Patient Record Systems

There are four main electronic patient record systems (EPRS) in use by the Trust:

- Lorenzo – used across the trust as a Patient Administration System (PAS) holding full demographic and, where available, familial data. The primary purpose is to collect referral, activity, inpatient, discharge, Care Programme and Mental Health Act data.
- SystemOne – this is an electronic clinical record that is a part of a key implementation project throughout the organisation. It holds the exact same detail as individual patient paper records and may be of a highly sensitive nature
- PC-MIS – is a web-based case management information system used by East Riding IAPT services.
- IAPTUS – this is an electronic clinical record for the veterans outreach service.

There are other Trust electronic record systems deployed or in deployment which may at some point take a data feed from the above systems. The enactment of this procedure acknowledges that these solutions are an integral part of trust business and thereby an individual cannot consent to their information being recorded on a core system (e.g. Lorenzo or SystemOne) yet dissent from it being used within one of the secondary Trust systems. These are (but not exhaustively listed):

- Trust Data Warehouse

Appendix 2: Patient Restriction on the Use of their Personal Information

Forename Surname

D.O.B. //

You are able to restrict how the Trust uses your information and who it is shared with. The Trust will respect such a restriction unless there are exceptional circumstances.

Please describe below how you wish to restrict the use of your information.

NAME:.....SIGNED.....DATE.....
(Patient)

NAME:.....SIGNED.....DATE.....
(Care Professional)

Please submit completed form to the Information Governance Team - hnf-tr.igteam@nhs.net

Copies for: -

- Patient
- Scanned in to Electronic Health Record

Appendix 3 – Flow chart to assess current and ongoing data disclosures

