INFORMATION SHARING PROTOCOL

# SUMMARY SHEET

|  |  |
| --- | --- |
| **Title of Agreement** | **Use of MSE Acute Care Portal for external clinical care purposes** |
| **Organisation Name** | **Head Office Address** | **Phone** | **Email** | **Named Data Protection Officer** | **ICO Notification reference** |
| Mid and South Essex Hospitals NHS Foundation Trust | Prittlewell Chase, Westcliff On Sea, Southend, Essex |  | mse.informationgovernance@nhs.net | Matt Barker | Z1972899 |
| Essex County Council | County Hall, Market Road Chelmsford, CM1 1QH  | 08457 430430 | dpo@essex.gov.uk | Paul Turner | Z6034810 |
| **Version Control** |
| **Date Agreement comes into force** | 03 April 2024 |
| **Date of Agreement review** | Annually |
| **Agreement owner (Organisation)** | Mid and South Essex NHS Foundation Trust |
| **Agreement drawn up by (Author(s))** | Matt Barker and Jane Marley |
| **Status of document – DRAFT/FOR APPROVAL/APPROVED** | Approved |
| **Version**  | 1.0 |

**Wider Eastern Information Stakeholders Forum**

This Information Sharing Protocol is designed to ensure that information is shared in a way that is fair, transparent and in line with the rights and expectations of the people whose information you are sharing.

This protocol will help you to identify the issues you need to consider when deciding whether to share personal data. It should give you confidence to share personal data

when it is appropriate to do so, but should also give you a clearer idea of when it is not acceptable to share data.

Specific benefits include:

* transparency for individuals whose data you wish to share as protocols are published here;
* minimised risk of breaking the law and consequent enforcement action by the Information Commissioner’s Office (ICO) or other regulators;
* greater public trust and a better relationship by ensuring that legally required safeguards are in place and complied with;
* better protection for individuals when their data is shared;
* increased data sharing when this is necessary and beneficial;
* reduced reputational risk caused by the inappropriate or insecure sharing of personal data;
* a better understanding of when, or whether, it is acceptable to share information without people’s knowledge or consent or in the face of objection; and reduced risk of questions, complaints and disputes about the way you share personal data.

Please ensure all sections of the template are fully completed with sufficient detail to provide assurance that the sharing is conducted lawfully, securely and ethically.

|  |  |  |
| --- | --- | --- |
| **Item** | **Name/Link /Reference** | **Responsible Authority** |
| Privacy Impact Assessment (PIA/DPIA) | ACP GP MSV1/STEWARDSHIP\_GUARDIANSHIP | MSEFT |
| Supporting Standard Operating Procedure | SOP/Guidance Doc/Individual User Agreement | MSEFT |
| Associated contract | N/A |  |
| Associated Policy Documents |  | MSEFT |
| Other associated supporting documentation | ACP GP Intergration Options Appraisal Report | MSEFT |

|  |  |  |
| --- | --- | --- |
| **1.** | **Purpose** | **REFERENCES** |
| Access to the ACP has been enabled to allow care professional and admin staff access to specific clinical information that is not available in their own clinical systems, to support patients on their care pathway. Access to information is needed to ensure accurate advice and care is given for specific patients speeding up (and removing blocks) to treatment.Essex County Council have requested access to the ACP to gain access to up to date and relevant information charting the progress of adults within their hospital journey that will inform ECC assessments and support timely discharge planning.  The Discharge to Assess Team works in partnership with our health colleagues at the hospital facilitating discharges from hospital via a number of pathways. Access to information held in the health portal will help ECC meet our duties under the Care Act i.e. assessment of need. The information will support ECC to correctly identify the correct pathway for discharge and ensure adult’s needs are met safely and effectively with the correct support in place where needed including timely access to the provision of occupational therapy and physiotherapy support.  | [GDPR](http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&rid=1)Go to article 5 |
| **2.** | **Information to be shared** |  |
|

|  |  |
| --- | --- |
| **Agency Name** | **Data field/description** |
| **Mid and South Essex NHS Foundation Trust** |  |

 | [GDPR](http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&rid=1)Go to articles 6 - 9 |
| **3.** | **Legal Basis** |  |
| **General Data Protection Regulation 2016 (GDPR) and Data Protection Act 2018.**

|  |  |
| --- | --- |
| **Personal Data** **(identifiable data)** | **Special Categories of Data** **(Sensitive identifiable data)** |
| Article 6:  | Article 9: (if appropriate):  |
| *Legal Obligation* | Health & Social Care |
| *Vital Interests* | Choose an item. |
| *Public Task* | Choose an item. |

Other legislation or statute as follows:* The Care Act with particular reference to section 3; Promoting integration of care and support with health services & Section 9 Assessment of Need
* The NHS Act 2006 with regard to Section 82; In exercising their respective functions NHS bodies (on the one hand) and local authorities (on the other) must co-operate with one another in order to secure and advance the health and welfare of the people of England and Wales.
* And in more broad terms; The Health and Care Act 2022 which seeks to promote collaboration and partnership-working to integrate services for patients.
 | [GDPR](http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&rid=1)Go to articles 6-14 |
| **4.** | **Responsibilities** |  |
|

|  |  |  |
| --- | --- | --- |
| For the purposes of this Protocol the responsibilities are defined as follows: For help go to [this link](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN) and see Articles 24 – 29 where these roles are explained. | Tick box | Organisation Name(s) |
| The Sole Data Controller for this sharing is: |[x]  Mid and South Essex NHS Foundation Trust(for data held on the ACP)ECC (for data recorded on SCCM) |
| The Joint Data Controllers for this sharing are: |[ ]   |
| In the case of **Joint Data Controllers**, the designated single contact point for Individuals is: |[ ]   |
| Data Processors party to this protocol are (please list): |[ ]   |

This Protocol will be reviewed one year after it comes into operation to ensure that it remains fit for purpose. The review will be initiated by **Head of Information Governance & Data Protection Officer, MSEFT** | [GDPR](http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&rid=1)Go to articles 13-14, 24 - 31 |
| **5.** | **Subject Rights** |  |
| Essex Partner Agencies’ Information Sharing Agreements are made publicly available on the Whole Essex Information Sharing Framework website to enable compliance with article 12 of the GDPR. It is each Partner’s responsibility to ensure that they can comply with all of the rights applicable to the sharing of the personal information. It is for the organisation initiating the ISP to identify which rights apply, and then each Partner to ensure they have the appropriate processes in place.

|  |  |
| --- | --- |
| **Subject Rights****Select the** [**applicable rights**](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/) **for this sharing according to the legal basis you are relying on** | Processes are in place to enact this right - please check the box |
| GDPR Article 13&14 – **Right to be Informed** – Individuals must be informed about how their data is being used. This sharing must be reflected in your privacy notices to ensure transparency. |[x]
| GDPR Article 15 – **Right of Access** – Individuals have the right to request access to the information about them held by each Partner |[x]
| GDPR Article 16 – **Right to Rectification** – Individuals have the right to have factually inaccurate data corrected, and incomplete data completed.  |[x]
| GDPR Article 17 (1)(b)&(e) – **Right to be forgotten** – This right may apply where the sharing is based on Consent, Contract or Legitimate Interests, or where a Court Order has demanded that the information for an individual must no longer be processed. Should either circumstance occur, the receiving Partner must notify all Data Controllers party to this protocol, providing sufficient information for the individual to be identified, and explaining the basis for the application, to enable all Partners to take the appropriate action. |[x]
| GDPR Article 18 – **Right to Restriction** – Individuals shall have the right to restrict the use of their data pending investigation into complaints.  |[ ]
| GDPR Article 19 – **Notification** – Data Controllers must notify the data subjects and other recipients of the personal data under the terms of this protocol of any rectification or restrict, unless it involves disproportionate effort. |[x]
| Article 21 – **The Right to Object** – Individuals have the right to object to any processing which relies on Consent, Legitimate Interests, or Public Task as its legal basis for processing. This right does not apply where processing is required by law (section 3). Individuals will always have a right to object to Direct Marketing, regardless of the legal basis for processing. |[ ]
| Article 22 – **Automated Decision Making including Profiling** – the Individual has the right to request that a human being makes a decision rather than a computer, unless it is required by law. |[ ]
| **Freedom of Information** (FOI) Act 2000 or **Environmental Information Regulations** (EIR) 2004 relates to data requested from a Public Authority by a member of the public. It is best practice to seek advice from the originating organisation prior to release. This allows the originating organisation to rely on any statutory exemption/exception and to identify any perceived harms. However, the decision to release data under the FOI Act or EIR is the responsibility of the agency that received the request. |[ ]

 | [GDPR](http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&rid=1)Go to articles 12 – 15[GDPR](http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&rid=1)Go to article 16 & 22 |
| **6.** | **Security of Information** |  |
|

|  |
| --- |
| **Security measures in place** |
| There are good quality access control systems in place |[x]
| Paper information is stored securely |[ ]
| Paper and electronic information is securely destroyed with destruction log for electronic information |[x]
| Laptops and removable media such as memory sticks are secured when not in use |[x]
| Technical security appropriate to the type of information being processed is applied |[x]
| Arrangements are in place to meet the requirements for confidentiality, integrity and availability |[x]
| Disaster recovery arrangements are in place |[x]
| Encryption of personal data is fully implemented |[x]
| Data minimisation has been considered |[x]
| Can pseudonymised or anonymised data be used to meet your processing needs? |[ ]
| There are sufficient access controls for systems/networks in place |[x]
| Routine and regular penetration tests are carried out |[x]
| Article 40 Codes of Conduct are adhered to (where applicable) |[x]
| Appropriate security is applied to external routes into the organisation; for example, internet firewalls and remote access solutions |[x]
| Confirm entry in Records of Processing Activity |[x]
| Auditing  |[ ]
| Signed Terms and Conditions of Use |[x]
|  |[ ]
|  |[ ]
|  |[ ]

Personal information will be securely shared viaAcute Care Portal electronic systemPartners receiving information will:* Ensure that only those employees who require legitimate access to the ACP are prioritised, as licenses are limited availability;
* Ensure that their employees read, understand and agree to the Terms and Conditions of Use for accessing the Acute Care Portal (ACP) prior to logging on to the system;
* Ensure that their employees are appropriately trained to understand their responsibilities to maintain confidentiality and privacy;
* Protect the physical security of the shared information;
* Restrict access to data to those that require it, and take reasonable steps to ensure the reliability of employees who have access to data, for instance, ensuring that all staff have appropriate background checks;
* To access only the information of those patients to whom you have a legitimate relationship;
* Not to share or disclose log-on details (Username and Password) with anyone;
* To be aware that electronic systems that access, process or transfer data are monitored on a continuous basis by the Trust. Any breach of security or infringement of confidentiality may be regarded as serious misconduct, which would lead to disciplinary action and potentially be escalated to the relevant professional body;
* Maintain an up to date policy for handling personal data which is available to all staff;
* Have a process in place to handle any security incidents involving personal data, including notifying relevant third parties of any incidents.

**International Transfers (Where applicable) – Not applicable** | [GDPR](http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&rid=1)articles 30 - 45 |
| **7.** | **Format and Frequency** |  |
| The format the information will be shared in is: | Electronic System (Acute Care Portal) |
| The frequency with which the information will be shared is: | Ad-hoc as needed |
| **8.** | **Data Retention** |  |
| Information will be retained in accordance with each partners’ published data retention policy available on their websites, and in any event no longer than is necessary.  | [GDPR](http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&rid=1)Go to article 5 |
| **9.** | **Data Accuracy** |  |
| Please check this box to confirm that your organisation has processes in place to ensure that data is regularly checked for accuracy, and any anomalies are resolved [x]  | [GDPR](http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&rid=1)Go to articles 5, 16 - 18 |
| **10.** | **Breach Notification** |  |
| Where a security breach linked to the accessing of data under this protocol is identified the Data Protection Officer for MSEFT, CCG and Partner organisations must be informed within 48 hours of the breach being detected. The email addresses on page 1 should be used to contact the Partners. The decision to notify the ICO can only be made after consultation with any other affected Partner to this protocol, and notification to the ICO must be made within 72 hours of the breach being detected. Where agreement to notify cannot be reached within this timeframe, the final decision will rest with the Protocol owner as depicted on page 1 of this document.All involved Partners should consult on the need to inform the Individual, so that all risks are fully considered and agreement is reached as to when, how and by whom such contact should be made. Where agreement to notify cannot be reached, the final decision will rest with the Protocol owner as depicted on page 1 of this document.All Partners to this protocol must ensure that robust policy and procedures are in place to manage security incidents, including the need to consult Partners where the breach directly relates to information shared under this protocol. | [GDPR](http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&rid=1)Go to articles 33, 34, 77 - 84 |
| **11.** | **Complaints** |  |
| Partner agencies will use their standard organisational procedures to deal with complaints from the public arising from information sharing under this protocol. | [GDPR](http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&rid=1)Go to articles 16 – 22 & 77 |
| **12.** | **Commencement of Protocol** |  |
| This Protocol shall commence upon date of the signing of a copy of the Protocol by the signatory partners. The relevant information can be shared between signatory partners from the date the Protocol commences. |
| **13.** | **Withdrawal from the Protocol** |  |
| Any partner may withdraw from this Protocol upon giving 4 weeks written notice to the Head of Information Governance & Data Protection Officer, MSEFT. The Partner must continue to comply with the terms of this Protocol in respect of any information that the partner has obtained through being a signatory. Information, which is no longer relevant, should be returned or destroyed in an appropriate secure manner. |
| **14.** | **Agreement** |  |
| This Protocol must be approved by the responsible person within the organisation (i.e. SIRO/Caldicott Guardian/Chief Information Officer). Signed copies should be retained by the Lead Organisation for the lifetime of the Protocol plus two years.

|  |  |
| --- | --- |
| Approver Name | Nicole Wood |
| Organisation Name | Essex County Council |
| Nominated Lead for Maintanance of User List | Nikki Jones |
| Approver Name | Matt Barker |
| Organisation Name | MSEFT |
| Date of Agreement  | 03 April 2024 |

**Please submit this Protocol to** **mse.informationgovernance@nhs.net** **with list of approved signatories.**  |
|  |