**Supporting Information for the Medicines Management Team Data Sharing Agreement (MMTDSA) 2021**

**Is there a Privacy Notice in place, covering the information to be shared?**

[x]  Yes - [Privacy Notice](http://www.doncasterccg.nhs.uk/about-us/fair-processing-data-protection-and-caldicott/?doing_wp_cron=1589530524.3845360279083251953125). The CCG have their own privacy notice which can be accessed here but as the GP Practice is the data controller of the patient information, they should ensure their own privacy notices reflect this Data Sharing Agreement. The Pharmacists and Pharmacy Technicians will be working on behalf of the Data Controller.

[ ]  No – please consider the need to create a notice

**Are you:**

[ ]  Collecting new personal data items that have not been collected / shared before?

[ ]  Introducing new or changing identity authentication requirements which may be intrusive?

[ ]  Introducing new privacy invasive technologies?

[ ]  Updating current or providing new links with data in other collections?

[ ]  Changing the medium for publically available information to enable data to be more readily acceptable?

[ ]  Converting transactions from anonymised/pseudonymised data to identifiable transactions?

[ ]  Changing a data delivery method that may be unclear or intrusive?

[x]  None of the above

***If you have ticked any boxes above, there is a requirement for the host organisation to update/amend their Privacy Notice.***

Please provide details below:

**What is the legal gateway for sharing?**

If relying on consent to share, please specify “Not applicable”.

A legal gateway is any piece of legislation which requires or allows the movement of information from one organisation to another. It may place a statutory duty on the organisation or powers on behalf of the individuals concerned.

|  |
| --- |
| UK GDPR Article 6.1(e), 9.2(h) |

**What information is being shared?**

[x]  Personal

**What is the lawful basis for processing (Article 6, GDPR)?**

[x]  Public task

**What is the lawful basis for processing (Article 9, GDPR)?**

Special category data **only**: race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life, and sexual orientation.

[ ]  Not applicable (personal data or statistical data only)

[ ]  Consent

[ ]  Obligations in connection with employment

[ ]  Vital interests

[ ]  Legitimate activities of a not for profit body or association

[ ]  Information has been made public by the data subject

[ ]  Necessary in relation to legal rights

[ ]  Necessary for public functions

[x]  Necessary for medical purposes

[ ]  Necessary for reasons of public interest in the area of public health

[ ]  Necessary for archiving purposes

**What is the lawful basis for processing criminal offence data (Article 10, GDPR)?**

Criminal allegations, proceedings or convictions **only**.

[x]  Not applicable

**What are the benefits to sharing the information?**

|  |
| --- |
| The interaction of the MMT will assist practice to adapt to the latest quality and safety developments, as well as prescribe cost effectively with limited impact on practice resources, compared to having to supply the time and expertise in house. This will maximise the effective use of resources for the patients of Doncaster. |

**Which data fields/items will be shared?**

Please list, for example name, address, telephone number, date of birth, etc.

|  |
| --- |
| **All fields may require access**  |

**In what format is the data being transferred and how?**

[x]  Electronic data – accessed on site by staff working for partner organisations

**Further notes on the above:**

|  |
| --- |
| Access to a medicines management folder on the practice shared drive is the recommended storage location.  |

**Information storage location**

[x]  Practice shared drive (recommended)

[x]  Paper folder in practice

[ ]  Encrypted memory stick

**What is the frequency of the transfer?**

[x]  Ad hoc

**Further notes on the above:**

|  |
| --- |
|       |

**How many records are being transferred?**

|  |
| --- |
| **Record numbers depend on the results of relevant audits** |

**Who are the data subjects?**

|  |
| --- |
| Patients  |

**Where will the information be stored by the receiving organisation after transfer?**

[x]  Server – system on organisation premises

[x]  Secure storage off organisations premises

**Further notes on the above:**

|  |
| --- |
| * Daily Server back up
* Full system backup is server wide (all hardware)
* Backup encrypted and stored on a separate network through active directory – Roles and responsibility required to access
* Main Server held on site and backup server held off site
 |

**How will the information be secured by the receiving organisation?**

[x]  Password protection

[x]  Smartcard/system password

**Further notes on the above**:

|  |
| --- |
|  |

**How will the information be accessed by the receiving organisation?**

[x]  System login

|  |
| --- |
| Can be audited |

**Further notes on the above:**

|  |
| --- |
|       |

**Who will access the information being shared in the receiving organisation?**

[x]  Employees – professional qualified staff

**Further notes on the above:**

|  |
| --- |
| **All staff are subject to annual re-validation, on appointment referencing, annual clinical supervision and DBS on appointment. At any time a DBS certificate number can be requested to view whether there have been any changes to the certificate data since appointment.** |

**How will the information be kept up to date and checked for accuracy and completeness by the providing organisation?** Select all that apply.

[x]  Assurance in place (e.g. IGT, PSN)

[x]  Staff aware of responsibilities when working with data

[x]  Clear retention schedules

**Further notes on the above:**

|  |
| --- |
| **Staff are contractually obligated to comply with the above measures.** |

**Describe your management of the retention and disposal of data by the providing organisation:** Select all that apply.

[x]  Assurance in place (e.g. IGT, PSN)

[x]  Policies and procedures in place which state/define retention schedules

[x]  Policies and procedures in place which state/define disposal methods and criteria

**Further notes on the above:**

|  |
| --- |
| Access is required as long as practices provide permission and an active DSA is in place. The CCG’s retention is in line with the [Records Management Code of Practice for Health and Social Care 2016](https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016) |

**Describe how you deal with Subject Access Requests for individual records and how you rectify / block / erase / destroy as necessary by individual request or court order by the data controller (host organisation):** Select all that apply.

[x]  Assurance in place (e.g. IGT, PSN)

[x]  Clearly defined procedures in place for Subject Access Requests for individuals

[x]  Clearly defined procedures in place to handle rectification and blocking of data

**Further notes on the above:**

|  |
| --- |
| The CCG and Doncaster GP Practices are responsible for responding to Subject Access Requests for the data, including complaints, should any be received. If the CCG receives a request, they will acknowledge receipt of the request, and advise the patient of whom is dealing with that request. The CCG is not able to respond to any requests where patient data is not re-identifiable. The CCG will not release the information to any third party without obtaining the express written authority of the partner who provided the information. |

**Describe the receiving organisation's policies, processes and standard operating procedures:** Select all that apply.

[x]  Assurance in place (e.g. IGT, PSN)

[x]  Clearly defined

[x]  Up-to-date

[x]  Readily available

[x]  Understandable (in plain English) for staff to use

**Further notes on the above:**

|  |
| --- |
| The CCG has an adequate Information Governance Framework and Data Quality Policy in place: [General policies](http://www.doncasterccg.nhs.uk/about-us/public-information/policies-and-procedures/general-policies/). The CCG are Cyber Essentials Plus.  |

**Describe the receiving organisation's management of incidents:** Select all that apply.

[x]  Reviewed, including any root cause analysis and action plans

**Further notes on the above:**

|  |
| --- |
| The CCG has an:* Incident management in place for if the hardware (server) being impacted resulting in major loss of data. Mechanisms embedded for loss of data with full restore options available for retrieval, as per RDaSH IT Policies and Procedures.
* Incident Management Policy. This details the requirements of the Information Governance Team to undertake a review and report the outcome of an incident to the providing organisation, the DCCGs Information Governance Group and the Executive Committee.
 |

**Describe the receiving organisation's training for both the system and data:** Select all that apply.

[x]  Assurance in place (e.g. IGT, PSN)

[x]  Users are aware of their responsibilities when using the asset

[x]  Regularly trained and tested on their understanding

[x]  Understand what to do in the event of a breach or incident

[ ]  Other – please specify:

**Further notes on the above:**

|  |
| --- |
| NHS statutory and mandatory training is undertaken by all CCG staff. Additional training for MMT staff is managed by the Head of Medicines Management  |

**Describe the receiving organisation's security of the asset:** Select all that apply.

[x]  Assurance in place (e.g. IGT, PSN)

[x]  Secure connection (e.g.https:)

[x]  Secure access (e.g. password protected)

[x]  Secure encrypted device (e.g. data stick)

[x]  Managed so only authorised persons can access and access routinely checked

[x]  Audit trail of interactions

**Further notes on the above:**

|  |
| --- |
| The CCG are responsible for adhering to the [records management code of practice for health & social care 2016](https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016)  |

**Describe the receiving organisation's business continuity arrangements:**

Select all that apply.

[x]  Assurance in place (e.g. IGT, PSN)

[x]  Clear business continuity arrangements

[x]  Users are aware of arrangements and appropriately trained

[x]  Regularly reviewed and updated (at least annually)

**Further notes on the above:**

|  |
| --- |
| The CCG has a Business Continuity Policy in place, with each department having their own detailed plans.  |

**Describe the receiving organisation's disaster recovery arrangements:**

Select all that apply.

[x]  Assurance in place (e.g. IGT, PSN)

[x]  Regularly reviewed and updated (at least annually)

[x]  Electronic part of a disaster recovery testing regime, regularly tested

**Further notes on the above**:

|  |
| --- |
| * Daily Server backed up by RDaSH on a daily basis
* Full system backup is server wide (all hardware)
* Backup encrypted and stored on a separate network through active directory – Roles and responsibility required to access
 |

**Does the third party/supplier agreement/contract(s) contain all the necessary Information Governance clauses regarding Data Protection and Freedom of Information?**

[x]  Not Applicable

**Further notes on the above:**

|  |
| --- |
|       |

**Review cycle:**

[x]  1 year