## Norwich Home Visiting Service – Information Sharing Protocol

This protocol sits beneath the Network Contract Directed Enhanced Service Data Sharing Agreement: Norwich Primary Care Network. The overarching agreement identifies best practice for systematic data sharing of health and social care information between signatories and this Information Sharing Protocol intends to provide granular detail of specific sharing initiatives agreed to by the parties involved.

|  |  |  |
| --- | --- | --- |
|   |   |   |
| Name of Project |   | Norwich Home Visiting Service |
|   |   |  |  |
| Description of Routine Sharing Practice |   | The purpose of this project is to support practices with home visits for adult house bound patients that are non-palliative, in a domestic setting and not under the care of a community matron. This document provides granular detail of this particular activity and acts as guidance on how to share information lawfully and appropriately between the signatories. 1. A patient is triaged as falling within scope of the Home Visiting Service (HV) by a Norwich practice
2. The practice completes a HVS Clinical Template within their own clinical system which then allows an Electronic Referral to be generated in SystmOne
3. EReferral will provide demographics of patient and reason for referral
4. Prior to the home visit, the HVS will access the full health record of the patient, which is able to be accessed from the HVS clinical system once a referral has been received
5. During the visit, HVS Clinician will enter the consultation in the patient’s record. This will automatically be visible to the practice once the record is saved
6. Following the home visit, the HVS clinician will relay any further actions to the practice for completion (including but not limited to, referrals to other services (such as NCHC, NEAT, NNUH, GP, Pharmacist), medication, follow up visits, blood tests)
 |   |
|   |   |   |   |
| Agreed Data Set |   | Patient demographics and referral informationFull patient clinical record |   |
|   |   |   |   |
| Preferred Secure Transfer Method 1 (SystmOne) |   | Record remains in situAccess via Smartcard |   |
| Preferred Secure Transfer Method 2 |   | NHS Mail / Telephone  |
| Other Methods |  |  |
|  |  |  |
| Secure Storage |  | Records remain in situAccess via SmartCard |
|   |
| Retention Periods |  | Practices involved in the arrangement should maintain proper audit trails of activities undertaken during the arrangement in the usual way |  |
|  |  |  |  |
| Legal Relationships |   | The process will involve sharing information from one Controller to another.“Where the same personal data is processed by a series of parties in sequence, each using the data for a different purpose then they will remain separate controllers ...” (ICO Guidance) |   |
|   |   |   |   |
| Fair Processing / Right to Be Informed |  | In order to satisfy the common law duty of confidentiality and the data protection legislation “right to be informed” there is a requirement to ensure that patients are provided with sufficient information. Individuals must “reasonably expect” disclosures of their confidential information.The parties must each include information about this initiative in their privacy notices and displayed in situ at all premises that provide information about their rights – including their right to object.Where a patient is being referred to other services following a home visit, they should be informed of the disclosure of information and any objections must be documented and handled with the support of the DPO**Due to COPI, there is no need to notify patients of this change however -if you notify your DPO of the arrangement, we can amend your website materials.**  |
|  |  |  |
| Data Security |  | All signatories must;* Have had data security and protection training within the last 12 months
* Have confidentiality clauses within their employment contract
* Have regard for internal protocols
* Make sure that any computer screens used to access the exchange cannot be seen by anyone who does not need to know.
* Ensure that screens are locked when away from desk
* Ensure that remote working practice complies with policies and procedures.
* Take responsibility for keeping Personal Confidential Information secure and confidential whilst working remotely, including preventing incidental access by others in the environment
* Not access any family, friend or colleague record unless absolutely necessary and manager notified

Additionally, staff should adhere to the following when remote working:**Using own laptop:**1. Avoid downloading software or videos / open suspicious links
2. Undertake all system / software updates
3. Ensure that the device has up to date antivirus software: Avast / AVG and malware bytes
4. Do not use a communal laptop
5. Where provided use software such as Away from my desk?
6. Do not print out documents on home printer, instead store in shared drive
7. Log out of all software and systems, including emails, when not in use
8. Within NHS Mail, only view documents in browser and do not download
9. Where possible create a normal “user” account on the laptop without admin capabilities to undertake the work
10. no documents should be downloaded to the laptop unless absolutely necessary, attachments to emails can be viewed in browser but there may other systems or portals accessed that permit the download of documents.

**Use of personal mobile phone:**Where limiting or prohibiting face to face appointments, it may be necessary for clinicians to conduct telephone appointments with their patients or for administrative staff to triage patients; both using their personal telephones. In this example, the only information input into the phone would be the patients’ number with no correlating personal data. Therefore, the risk to the data is relatively low. Practice should issue the following instructions to support secure working on personal laptops. 1. Do not store patients’ names against phone numbers
2. Delete call log daily / weekly
3. Do not allow anyone else to use phone (unless cleared of work-related data)
4. If accessing emails download a free antivirus – Avast / AVG
5. Check permissions settings on all apps downloaded onto phone and **turn off** access to phonebook / call log (Facebook / WhatsApp)
6. Do not undertake phone calls with family in the same room, if possible, use headphones instead of speakerphone.
 |
|  |  |  |
| Lawful Basis  |   |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Purpose** | **DPA 2018 (personal data)** | **DPA 2018 (special cat)** | **GDPR (personal data)** | **GDPR (special cat)** | **ECHR Art 8** | **Common Law Duty of Confidentiality** |
| Direct care to individual | Sch 9 s 5 (e) Public Task | Sch 10 s 10 8(1) Medical Purposes | Art 6 (1) (e) Public Task | Art 9 (2) (h) Medical Purposes | In accordance with the lawProportionate | Duty set aside by Regulation 3 (4) of the Health and Service Control of Patient Information (COPI) Regulations 2002  |

 |

|  |  |  |
| --- | --- | --- |
| Patient Right to Object (Information Sharing Scripts) |  | **N/A** |

|  |  |  |
| --- | --- | --- |
| Incidents report to: |  | Emma Cooper, Practices DPO  |
| Access Rights Requests reported to: |  |  IG Lead for each practice |
| Approved by: |  | A copy of this document should be provided to… |
| Approval date:  |  | 6th May 2020 |
| Review date |  | 30th September 2020 |
| In case of queries about the content of this document contact: |  | Emma.cooper@kafico.co.uk |