## Cross PCN Working During COVID-19 Pandemic– Information Sharing Protocol

This protocol sits beneath the [insert name of overarching sharing agreement]. 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 |   | Cross PCN Working During COVID-19 Pandemic |
|   |   |  |  |
| Description of Routine Sharing Practice |   | The purpose of this project is to allow practices to provide support across the [insert] PCN with direct patient care activities during the current COVID-19 pandemic. This document provides granular detail of this particular activity and acts as guidance on how to ensure patient data is still protected and best practice on audits and reporting where necessary. 1. [insert] will nominate a list of their employed staff members to be provided with access to practice systems
2. Practices will confirm to RA Team that access may be provided to the nominated [insert] staff members
3. Access will only be for legitimate practice activities such as direct patient care, audit or disclosures to relevant bodies (Public health or 111 for example)
4. Incidents will be reported to the DPO for each practice – ie, if an incident occurs during [INSERT ORG NAME] access or processing of practice data, they will report to the DPO for that practice
5. [INSERT ORG NAME] will only use the provided access where the practice has provided express permission for that activity to take place

Some anticipated examples of access are;1. [INSERT ORG NAME] Pharmacists will receive Eclipse alerts under COVID Protect related to medication needs of at risk patients and will action these to support the patient (a full record of actions take will be made in the clinical record)
2. Clinical Directors will undertake activity reviews such as reviewing the activity of the Yellow Hub and making practices aware of any relevant patient updates
3. [INSERT ORG NAME] Physios will access a list of patients that have outstanding referrals and contact them to support ongoing management of their condition during the pandemic

[INSERT ORG NAME] must notify practices of when they intend to use the access that has been granted and for what purpose.Practices must continue to audit their systems for appropriate access as much as practical during this time. |   |
|   |   |   |   |
| Agreed Data Set |   | Full 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; including any COPI disclosures made |  |
|  |  |  |  |
| 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.**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 data 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.

It has been identified that there are limitations to the clinical systems’ ability to audit access to both appointment and tasks lists when working across organisations. This is compounded by the fact that cross organisational working might mean that staff members have inadvertent access to friends, families or their own information when present in a task or appointment list.There are currently limited ways to manage this risk (which will be raised with system providers) but parties are advised to;* Send the awareness message found at Appendix A to all staff who will be undertaking cross organisational access
* Make endeavours to notify patient population of the cross organisational access arrangements so that they can raise particular concerns about their information being accessed by someone from another practice
* Consider how to support when a patient does raise concerns as above
 |
|  |  |  |
| 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:  |  | TBC |
| Review date |  | 30th September 2020 |
| In case of queries about the content of this document contact: |  | Emma.cooper@kafico.co.uk |

## Appendix A

## Possible Staff Awareness Message

**Cross Organisational Access to Clinical Systems**

Cross organisational working might mean that staff members have inadvertent access to friends, families or their own information when present in a task or appointment list.

Where possible, please alert the practice manager if this is something you anticipate might happen (for example, you are aware of family members or friends registered at another practice).

Please remember that unauthorised disclosure of information obtained in this way is a criminal offence. Staff must exercise discretion and professionalism where information of this kind is inadvertently accessed through the system and not disclose outside the legitimate activities of your role.

## Possible Patient Awareness Message

**Cross Organisational Access to Clinical Systems**

Your practice is collaborating with other practices within our Primary Care Network during the COVID19 Pandemic. This means that staff from one practice may have access to records from another practice in order to support during these difficult times.

All staff continue to be bound by confidentiality and have had training in keeping your information secure.

If you have any concerns about your information being accessed by staff from the following practices, please contact us at XXXXX and let us know.

XXXXXXXXXX

XXXXXXXXXX

XXXXXXXXXX