DPO Cluster Quarterly Newsletter

# DECEMBER – JANUARY – FEBRUARY 2018 / 19

## What have we achieved so far?

As a cluster group, we have formed to allow joint working towards data protection assurance and to create a network of practices under a single Data Protection Officer.

So far, we have;

1. Created a Processing Activities Log 
2. Developed a deeper level of transparency for data subjects 
3. Developed Protocols to support data protection compliance 
4. Developed a cluster-wide approach to clinical system audit 
5. Undertaken Data Protection Impact Assessments for sharing initiatives
6. Created a master log of all sharing partners across the county
7. Undertaken a Data Security Compliance Audit
8. Raised awareness of Subject Access Requests through Webinars

## What was covered at the latest cluster event?

Subject Access Requests

* An up to date SAR protocol has been provided to support this activity [HERE](https://www.kafico.co.uk/policies-and-protocols)
* iGPR presented a free auto-redaction software available to practices
* A SAR Webinar has been delivered for all practice staff to support the process – recording available [HERE](https://www.kafico.co.uk/copy-of-policies-and-protocols)
* Practices are advised to reduce letter-sending and aim to send emails where possible – more secure and prompt route

Information Risk Management

* We have identified the processing activities that result in a **higher risk** to the rights and freedoms of data subjects
* You should highlight these to your practice SIRO and ensure that you have taken the identified actions

|  |  |
| --- | --- |
| Risk | Actions |
| CONFIDENTIAL WASTE DESTRUCTION | Our practice has identified this as a high-risk activity to the DPO. |
| The contract we have in place with our provider has been notified to the DPO for review  |
| We retain all certificates of destruction provided by our confidential waste provider |
| We ensure that confidential waste bins are secure and collected regularly |
| We monitor any incidents related to confidential waste destruction |
| PCSE NOTES | We monitor any incidents related to PCSE notes |
| We ensure that PCSE notes are stored securely and access is limited |
| REMOTE WORKING | Staff are provided with remote working protocols (these are included in IG08 Information Sharing and Privacy Protocol) |
| Staff are provided with secure connections for remote working (VPN) |
| All staff have had IG training in the last 12 months |
| DIABETIC EYE SCREENING | Our practice has instructed our DPO who has conducted a DPIA (complete) |
| NHS Health Checks | Our practice has instructed our DPO who has conducted a DPIA (complete) |

Introduction to Hannah Calway

* Studied Law with Business at Brighton University
* This included International and EU Law, Contract, TORT and Criminal Studies. Experience in Power of Attorney
* Hannah is the Point of contact for any Information Governance Incidents
* Any difficult SARS received can also be referred to Hannah
* She is checking new and existing processors for compliance
* She is responsible for customer audits, including upcoming SAR audit to check internal compliance and for arranging workshops

The Q3 cluster event also covered three themes.

Records Management

* RM is important for effective working, risk reduction, information rights, NHS Care Records Guarantee.
* Records must be created within clinical systems or stored in the shared network
* Records must not be stored in personal drives or mobile devices such as mobiles or memory sticks
* Try to name files in a logical way that is obvious to the user (e.g not “Dave’s spreadsheet”)
* Records must not be kept for longer then necessary for identified purpose(s)
* Department of Health RM Code identifies key retention periods for health and social care records
* DPO has provided a simple Key Record Retention Schedule [HERE](https://www.kafico.co.uk/policies-and-protocols)
* DPO has developed a simple process for regularly undertaking a records retention / management review at the bottom of the page [HERE](https://www.kafico.co.uk/policies-and-protocols)
* Destruction digital records must be in line with international standards - CSU should provide these to you when they collect hardware
* Paper records must be destroyed in line with NHS Digital Standards so do retain all certificates of destruction from your confidential waste service provider

Training and Awareness

* You should undertake an internal Training Needs Analysis. A template can be found at bottom of the page [HERE](https://www.kafico.co.uk/policies-and-protocols)
* ALL staff must have been trained in data security in the last 12 months – ICO always ask for evidence of this
* DPO has provided dates for Caldicot and SIRO training (optional)

Data Security Toolkit

* We went through the toolkit line by line
* A guide for completion was provided to all customers
* DPO actions will be completed in coming weeks
* DPO will continue to liaise with CCG / CSU for other evidence
* DPO will draft an agreement that System Administrators can sign to hold them accountable

## What is our DPO doing between now and the next event?

* Sending quarterly newsletter 
* Arranging SAR Webinars 
* Providing system list for toolkit evidence - **Pending**
* Providing contract list for toolkit evidence- **Pending**
* Creating cluster-wide policies and protocols to prevent the need for branding locally and to allow staff to access them directly within the Mydpo repository- **Pending**
* Risk review the systems where passwords are shared- **Pending**
* Produce an agreement that can be signed by System Administrators
* Add a section to the IG09 Information Incident Management protocol around unauthorised access to records

## What should our practice do before the next event?

* Undertaking regular access audits using the template provided by the DPO [Access Audit Template Here](https://1drv.ms/f/s%21AjHx1anZWPVX7C27vrGH-r_HpNcc)
* Responding to email instructions related to amendment of transparency materials (DPO to send)
* Ensuring staff have access to updated protocols
* Complete any actions sent by Hannah as a result of the Data Security Compliance Audit
* Undertake a records management review [HERE](https://www.kafico.co.uk/policies-and-protocols)
* Escalate risks identified above to SIRO and complete the identified actions

## incident Learning

Here is a roundup of learning from this and previous quarters from actual incidents across the cluster;

* Ensure that any old forms / templates / pro formas are removed from site and from computers. These sometimes have a footer that say “once complete, send this form to…..” This can result in personal data being sent to addresses that no longer exist and being opened by Royal Mail
* Ensure that postal addresses are redacted from records before being released as a SAR. This counts as personal data related to a third party and may relate to some one who does not want their address known. Such as an ex-partner.
* Lots of incidents where people have the same surname. Cross check other elements of the record before releasing information.
* When a staff member leaves their job and their email access is removed by the CSU, check they cannot use the “forgotten password” function to regain access remotely. This appears to be a loop hole that the CSU had not previously considered.
* If you receive report requests for using a third-party form, check them carefully to see whether the patient has ticked a box asking to view the report ***before*** they go to the employer / claims company etc. This can be missed.
* Do not use pre-set numbers in a fax machine (or better yet do not use fax machines)
* Ensure that envelopes are robust. When they are heavy or very full – apply tape to prevent them coming open at sorting office.
* Double check to ensure emails are being sent to the correct sharing partner each time
* Take the time to check the coding being placed on a patients file is correct. Incorrect coding can lead to patients being offered / missing out on services available to them.
* When printing documents, ensure you get them from the printer straight away and check they are 1. the documents you printed and 2. Related to this particular patient before handing them out.
* Ensure staff members only have the access they need for their particular role. Email access should be limited to only those who have to deal with them.

## What’s next?

The next cluster event will cover

Business Continuity and Disaster Recovery

Profiling and Auto Decision Making

Children and Young People

See you in April!