KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

NORFOLK DPO CLUSTER QUARTERLY NEWSLETTER

MARCH – APRIL – MAY 2019

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 ✓
9. Created a master log of all information assets / systems and risk scored them ✓

WHAT WAS COVERED AT THE LATEST CLUSTER EVENT?

The Q4 cluster event covered three themes.

Business Continuity

⇒ Business continuity obligations are both legislative (Civil Contingencies Act and Data Protection Act / GDPR) and driven by NHS commitments

⇒ National Data Guardian standards provide that Business continuity plans are in place and tested

⇒ Practice continuity plans must include critical information assets and response to cyber incident

⇒ CSU are biggest processor and therefore risk but no clear approach to Business Continuity

⇒ Practices would value more proactive approach to information risk and continuity from CSU

⇒ SIRO and CG should review the plans to ensure that they include information risks and the rights of patients (for example, providing comms in the event of large scale breach)

⇒ The workshop group conducted a risk assessment of Master System List to identify the high risk and high value assets for practices

⇒ DPO to summarise and send for inclusion in practice Continuity Plans

Profiling and Automated Decision Making

⇒ Profiling is automated processing of personal data to evaluate personal aspects relating to natural person

⇒ Practice examples include Frailty Index, Case Finding, CCG Risk Stratification

⇒ Automated decision making is making decisions by automated means without human intervention

⇒ There are risks of 'invisible processing' and inferred sensitive data.

⇒ Data protection law gives individuals the right not to be subject to solely automated decision making where it would have a legal or significant effect

⇒ Data protection law gives individuals the right to have the logic behind profiling explained to them

⇒ Practices **are** performing profiling but not automated decision making

⇒ Must be transparent about this in the notices and be prepared to explain the logic behind them

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

Children and Young People's Information

⇒ Children and Young People's information warrants special protection because they are vulnerable

⇒ The age at which children are considered competent to make decisions about their health information is younger than the age they can make decisions about their health care (12)

⇒ Younger children might also be assessed as competent to make decisions about their information

⇒ Unless there are concerns, such as abuse, Children's decisions to keep information from their parents should be respected

⇒ If considered to be in best interests of the child (risk of significant harm), disclosure may take place without child's consent

⇒ If a child makes a decision to disclose information and the parents object, parents should usually be informed that the disclosure will take place (unless this would breach duty of confidentiality)

⇒ If parents are requesting access to child's record and the child is competent, access should only be granted with child's consent

⇒ Access should not be granted to information where the child had an expectation of confidentiality (consider sexual health etc) unless in the best interests of the child (consider redaction)

⇒ Right to erasure particularly important for Children as they may not understand that sometimes they cannot change their mind. Must be fully explained.

⇒ Children have a human right to be protected from harm but also to autonomy and privacy

⇒ Disclosures under the Children Act must be factual and proportionate

⇒ Consent may not always be appropriate. In these cases, considering informing.

⇒ Informing may put child or others at risk.

⇒ Do not make promises of confidentiality that cannot be kept

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

WHAT IS OUR DPO DOING BETWEEN NOW AND THE NEXT EVENT?

⇒ Sending a Master Processing Activities Log ✓

⇒ Sending quarterly newsletter ✓

⇒ Arranging Incident Management Webinar

⇒ Adding SIRO report to Newsletters ✓

⇒ Write letter to CSU requesting proactive communication re information risk and business continuity

⇒ Send Children and Young People Rights slides out to cluster for dissemination

⇒ Add Children and Young People section to SAR Protocol

⇒ Provide an action plan for auditing third party access to clinical systems i.e. community

⇒ Add eReferrals to Master Systems List

⇒ Obtain list of profiled information (flags within clinical systems and Eclipse) and produce explanation of the logic to support response to information rights requests

INCIDENT LEARNING

Here is a quarterly round up of the learning from actual incidents across the clusters in the last quarter;

! 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.

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

- 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 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.

- Ensure that records are put away at the end of the day. A recent break in at a Norfolk practice resulted in media attention and concerned patients.

- Third party access to clinical systems must be considered when it comes to audit schedules. Recent incident involved third party accessing records inappropriately.

WHAT'S NEXT?

The next cluster event will cover

Information Sharing

Information Rights

Access Control and Audit

See you in July!

SIRO REPORT

Please forward this Newsletter to your SIRO to give them sight of this section which intends to link up the risk management activities of the DPO and the risk ownership of the SIRO.

Key Risks and Issues identified this quarter

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

Risk / Issue	Action for DPO	Suggested Action for SIRO
There is a risk that the Business Continuity Plan does not include critical assets or that the CSU has not provided a sufficient plan for incidents	Provide list of critical assets to be included in practice plan Engage CSU to develop better plan	Ensure that practice GDPR lead has incorporated critical assets into practice business continuity plan Ensure that practice GDPR lead distributes and actions the improved plan once received
There is a risk that the practice is not sufficiently transparent about profiling activities or prepared to provide information about the logic of such activities	Obtain list of profiling flags within clinical systems and Eclipse Produce confirmation of the logic applied to profiling ready to provide to patients on request	Ensure that when logic document is produced, staff are made aware of its relevance to information rights requests
There is a risk that staff are not adequately information about children and your people's information	Send Children and Young People Rights slides out to cluster for dissemination Add Children and Young People section to SAR Protocol	Ensure that GDPR lead distributes the materials to the appropriate staff within the practice
Recent incident highlighted that there is a risk that third parties accessing the clinical system might be doing so inappropriately	Provide an action plan for auditing third party access to clinical systems i.e. community	Ensure that once the action plan has been produced, it is effectively implemented by the GDPR lead