**The Northern, Yorkshire & Humberside**

**NHS Directors of Informatics Forum**

**Information Governance Sub-Group**

**Yorkshire & Humber Area Strategic Information Governance Network (SIGN)**

**Lecture Room, Goole & District Hospital, Woodland Avenue, Goole, DN14 6RX**

**Notes of the Meeting held on Friday 13th December 2019, 13:00 – 16:00hrs**

**P**res**ent:**

|  |  |  |
| --- | --- | --- |
| **Name** | **Initials** | **Organisation** |
| Susan Meakin (Chair) | SMe | NLaGH |
| Roy Underwood | RU | DBTH |
| Jo Higgins | JH | HDFT |
| Kay Hill | KH | HDFT |
| Joanne Robertshaw | JR | RDaSH |
| Lucy-Ann Boatman | LAB | HTFT |
| Tracey O’Mullane | TOM | HTFT |
| Barry Jackson | BJ | Embed |
| Steve Rose | SR | CHFT |
| Adam Mosley | AM | Schoen Clinic York |
| Susan Hall | SH | Audit Yorkshire |
| Caroline Squires | CS | Calderdale CCG |

**Apologies:**

|  |  |  |
| --- | --- | --- |
| Helen Harris | HH | Doncaster CCG |
| Derek Stowe | DS | TRFT |
| Jenny Pope | JP | Airedale and Bradford |
| Caroline Britten | CB | RDaSH |
| John Wolstenholme | JW | Sheffield Health & SC |
| Rachael Smith | RS | SWYT |
| Hannah Gregson | HG | BHFT |
| June Emptage | JE | Optum |
| Erin Wood | EW | Health Education England |
| Caroline Million | CM | Embed |
| Steve Creighton | SC | Leeds CCG |
| Shaun Beckingham | SB | Leeds CCG |
| Karen Rowe | KR | Leeds CCG |
| Andy Nutting | AN | Leeds City Council |
| Linda Da Costa | LDC | NLaGH |
| Matthew Washington | MW | SWY |
| Caroline Million | CM | Embed |
| Rachel Smith | RS | SWYT |
| Claire Attwood | CA | City Healthcare Partnership |
| Andy Thompson | AT | York Teaching Hospital |
| Dianne Llewellyn | DL | Mid Yorks |
| Martin Moorhouse | MM | Mid Yorks |

|  |  |  |
| --- | --- | --- |
|  |  | **Action** |
|  |  |  |
| 1 | Apologies - See above |  |
| 2 | Minutes of previous meeting held on 8th November 2019 – No Comments received so accepted as a true record. |  |
| 3 | Action points ( Paper B)  Action Point 8 – both TOM and SMe have approached NHS Digital regarding the IAO training that is currently being provided by Templar. SMe had received an email from NHS digital stating that the Trust would need to provide names, emails and job titles for each IAO and then this information would be passed to Templar for access to the training to be granted. SMe agreed to send the details out. See below  ***Post meeting note***  Below is from NHS D  ***IAO and Clinician Training***  *Further to the announcement in the September Highlights section around SIRO Training we are now able to offer the following on-line training modules: -*   * *IAO (Information Asset Owners) – we are happy for multiple IAOs per organisation with no limit on this as yet (large orgs can have multiple IAOs) – however, it is likely to have a limit attached once we have some feedback on its uptake. Online training (45mins long)* * *Clinicians – Online Training (45mins long)*   *Registration for this is via the* [*cybersecurity@nhs.net*](mailto:cybersecurity@nhs.net) *email and then a link to training tool will be provided.* | SMe |
| 4 | **DPIA’s**-  SMe enquired how members of the group defined what ‘High Risk’ processing is and if they are accepting DPIA’s for such processing only, or if they were accepting DPIA’s for any processing activities. Following discussion the group felt that restricting DPIA’s to only ‘High Risk’ processing would potentially be detrimental to the work that had already taken place within organisations to encourage staff to complete DPIA’s. The group felt it was better to receive all DPIA’s irrespective of risk, than none at all. It was agreed that maybe the screening questions needed to be broken down to identify which were ‘High Risk’. Each organisation to take this away. |  |
| 5 | **Regional/National Events update**  YHCR workshop for Information Governance, Clinical and  Social Care Practitioners – 03/12/2019  Member of the group who attended said they felt it wasn’t very informative and did not cover fundamental IG issues in-depth for example audit trails. Those that attended were still awaiting copies of the slides. |  |
| 6 | **IG Education/Personal Development Updates**  **Cyber Training for IG Professionals.**  SMe was aware of ‘Cyber Training for IG Professionals’ provided by Act Now which a member of Doncaster Council had attended, the feedback received was good.  BJ informed the group of an NHS E/I WebX on the Secondary Use Data Governance Tool which he had participated in and that it contained relevant and useful information the tool can be found via the following link.  <https://data.england.nhs.uk/sudgt/> |  |
| 7 | **EU Exit/Brexit**  31 Jan 2020 – nothing to report. |  |
| 8 | **Data Security and Protection Toolkit**   |  |  |  |  | | --- | --- | --- | --- | | 6.3.5 | Known vulnerabilities are acted on based on advice from CareCERT, and lessons are learned from previous incidents and near misses. | **Are all new Digital services that are attractive to cyber criminals for the purposes of fraud, implementing transactional monitoring techniques from the outset?** | Includes an assessment of which services are susceptible to fraud, if none respond No services attractive to fraud. |   CS asked how members were taking the above assertion.  SMe asked if organisations had approached Fraud departments to provide input to this assertion. The response was split through the group. The group discussed the use of card payment facilities, eg coffee shops, parking, pharmacies (third party), timesheets, pay systems.  TOM stated that they had assessed the E-expense system however like most organisations were struggling with resource to undertake access audits.  SH noted that the toolkit states ‘new’, therefore only new digital services need to be assessed and not done retrospectively. DPIA’s and contracts would be suitable forms of evidence.  However consideration of historic systems which are deemed a ‘high risk’ and appropriate assessments completed.   |  |  |  |  | | --- | --- | --- | --- | | 6.3.5 | You have demonstrable confidence in the effectiveness of the security of your technology, people, and processes relevant to essential services. | **Your confidence in the security as it relates to your technology, people, and processes has been demonstrated to, and verified by, a third party in the last twelve months.** | For example, as a minimum, using an Onsite Assessment by NHS Digital and other relevant services that form part of NHS Digital’s Cyber Security Support Model (please see www.digital.nhs.uk/datsecuritycentre). CCGs may be covered by their CSU assessment) |   CS also raised the above assertion.  There were a number of assessments which Trusts were using as evidence there ranged from completing the Cyber Security Resilience Check by NHSD, obtaining Cyber Essentials Plus.  <https://digital.nhs.uk/services/data-security-centre>  **Approaches to Data Protection by design.**  SH informed the group that Audit Yorkshire is developing common understanding with other auditors (360/AuditOne) re toolkit big picture guides and tool tips. Members need to remember that the tool tips give examples and that these are not exhaustive. The ICO Data Protection by Design checklist is very useful and Trust may find is useful to incorporate in to spot check audits.  ***Post meeting note, clarification received from John Hosdon, NHSD.***  On DP by Design it is designed to be as it says on the tin. An audit has been undertaken it needs to cover the items listed in the tooltip i.e. This should be In the last twelve months, covering access control, encryption, computer port control, pseudonymisation and physical controls.  For the audit pilot we developed further details to support internal auditors, which some orgs have found helpful if they are struggling on understanding what documentation etc to produce.  Link <https://www.dsptoolkit.nhs.uk/Help/64>.,  Control Objective  The organisation has undertaken an internal audit to assess their compliance with the GDPR's data protection by design requirements.  Approach  1. Request to review a copy of the latest data protection by design audit report. Has the audit been completed within the last 12 months?  2. Has the audit identified clear remediation actions (where applicable), with identified individuals accountable for remediation actions and clear time scales for completing them?  3. Has the audit report been approved/signed off by the organisation's board / audit and risk committee (or equivalent)?  4. Has progress against the action plan identified been monitored and reported on to the organisation's board or similar committee, meeting or group with representation from the organisation's senior management?  Request evidence to demonstrate this assertion.  Assessment Documentation 1. Copy of an audit report that has considered data protection by design practices and related risks within the last 12 months.  2. Relevant documentation or evidence to demonstrate that any actions arising from the audit are reported on and monitored by the organisation's board or similar committee, meeting or group with representation from the organisation's senior management.  TOM enquired if anyone else had or is going to be undertaking a three tier audit this year, which would identify gaps in previous audits and then only concentrate on found gaps. TOM has found the different approach very long winded. General consensus was that the 2 tier approach was one that has and is being used. |  |
| 9 | **Confidentiality, Data Protection and Freedom of Information**  **Transgender Records**  SME informed the group that NHSX are drafting national guidance. A number of members stated that they had already developed their own guidance and would be interested to compare when it is released. A discussion took place around current processes in place which covered the recording/merging and recording within such records and around certification of transgender.  **Inter-Agency Information Sharing Protocol.**  Chair raised on behalf on Rachael Smith (SWYFT). If anyone signed up knew if there was an updated version. RS to respond directly to Rachael Smith. | RS |
| 10 | **Data and IT/Information Security**  **How do organisations using NHS Professionals or temporary/locum staff manage Active Directory accounts in relation to access the clinical systems – raised by Dianne Llewellyn**  There were different processes across organisations, these ranged from;   * Having site managers available to provide access to systems when required. * Issuing temporary cards – raising Datix to record that card/access is issued then retrieve card. * Ensuring agencies are aware of process of access and return of cards so agency staff have time to obtain cards. * Temporary cards are issued and retrieved by switchboard as they are open 24hours. * Staff should have a smart card if a regular locum, however if not, a temporary locum card is issued and logged to enable auditing. The locum is required to leave a deposit which is returned when the card is handed back.   **Network and Information Systems Regulations Survey**  SME raised for information only that a Survey had been sent out to organisations. A number of members were aware  **“A five-year framework for GP contract reform to implement The NHS Long Term Plan*”***  *• Para 5.10 (ii) The Bold is NHS E’s*  *• all patients will have online access to their full record, including the ability to add their own information, as the default position from April 2020, with new registrants having full online access to prospective data from April 2019, subject to existing safeguards for vulnerable groups and third party confidentiality and system functionality*  Discussion took place especially around the terminology of “prospective” and “all” records and also around “Lloyd George” (packets containing paper records - historic), and the resources to make these available electronically for current registrants (ie retrospectively).  BJ said his GP practices have been made aware for years to scan the “packets” so an electronic record is retained and destroy the paper copy, this removes any duplication and therefore clinical risk. Also noted that they have a policy/guidance for staff that anything within the “packet” /electronic record that are contains information that could be harmful or contain third party, are noted on system/reviewed by clinicians in real time, so that they are not displayed within the record online. Agreed to share policy/guidance. |  |
| 11 | **AOB**  • SR – what do other orgs do with return addresses on correspondence?  Discussions highlighted that organisations use a mixture of HQ address/IG address or PO Boxes for return addresses.  • SR – old Police DP7/9 forms – does anyone know of a formal process for approving the new forms under new legislation. Discussion highlighted as long as the legal basis explanation was clear, this was sufficient. RU made reference to GPR Article 23(1)(d). Still contained countersignature if consent was not provided. TO’M noted that she is aware of one form that provided “consent” for access/release of records, when in fact it was only a consent from the data subject to say that they had been given a copy of the Police’s privacy notice..!  • RU asked if anyone had a policy on videoing board meetings. His org has one for audio recording board meetings, and was inclined to get them to amend to include video. Discussion took place and the group felt at as this was a public meeting and as long as the public were made aware that it was being video recorded or live streamed, that was sufficient. However the Trust would need to consider their response, if a number of objections were received. |  |
|  | **Date and time of next meeting –**  Friday 10 January 2020, 13:00 – 16:00, Lecture Room, Goole and District Hospital, Woodland Avenue Goole, DN14 6RX |  |