Privacy Impact Assessment

|  |  |
| --- | --- |
| Title of Project, Process or Initiative | CAFM (Computer-Aided Facility Management) System |
| Summary of Project, Process or Initiative | Installation and implementation of a CAFM system to run and monitor the Estates helpdesk and planned maintenance functions, as well as logging and monitoring portering, catering and domestic requests. |
| Directorate | Estates and Facilities |
| Client |  |
| Date | 16/05/2018 |
| Author |  |
| Version No | 1 |

# Guidance

|  |  |
| --- | --- |
| Why should I do a Privacy Impact Assessment (PIA)? | The principle behind PIA's is to look at the privacy risks associated with a new project or piece of work and to see if you can use less privacy invasive options. |
| When should I complete a PIA? | A PIA should be undertaken at the start of a project or initiative and certainly before equipment or services are purchased.  |
| Who should complete a PIA? | **Stage 1** below should be completed by project managers, leads for new initiatives and service commissioners / procurement managers. **Stage 2** below should then be completed with the Information Governance Team. |
| Who signs off PIAs? | The Information Governance Steering Group will review the completed PIA.  |
| Data Flow Mapping | The data flows identified in this PIA must be added to your departmental Data Flow Map. Contact your manager or the IG team to see your current map. |
| How should I record residual risk? | **Any residual risks identified after conducting this PIA must be added to your Corporate Risk Register. This PIA cannot be signed off until this has been completed.** |

## Definitions

|  |  |
| --- | --- |
| Person Data | All data about patients, public or staff is referred to as personal data This includes data that can **identify** a person as well as information **about** that person e.g. health or staff records. |
| Anonymous record | All data that can potentially identify an individual, whether alone or in combination with other data, has been deleted. |
| Pseudonymised record | PID is replaced with a pseudonymised identifier. E.g. AB4878 replaces name. This must allow the new identifier to track back to the original record. Other examples. Address becomes Tonbridge, or Kent. Date of birth (26/12/74) becomes age 36. |

# Stage 1: Data Processing

|  |  |  |  | **To be completed for YES answers ONLY** |
| --- | --- | --- | --- | --- |
|  | Question | Guidance | Y/N | What changes are there? | What are the privacy risks? | How will you mitigate the risks? |
|  | Is new or additional technology being used that has substantial potential for privacy intrusion? | E.g. biometrics, surveillance, digital image recording, new statistical analysis & logging of electronic traffic. | N |  |  |  |
|  | Are new identifiers being introduced?Are existing identifiers being used for a new purpose?Could the purpose be construed as intrusive?  | E.g. violent patient crime numberE.g. postcode use for patient surveyE.g. facial recognition software | NNN |  |  |  |
|  | Might the status of anonymity or pseudonymity be changed or denied? | Will someone be identifiable where they could not be before? | N |  |  |  |
|  | Are multiple organisations involved? | Data Controller / Processor relationship must be explicit in contract and purpose for information sharing must be clearly documented  | Y | Change of provider of electronic “helpdesk” system for Portering and estates.Introduction of electronic system for other Facilities departments (cleaning, catering, transport)  | Staff names (no other information)Patient names may sometimes be used (already used on current Portertrac system) | Contract specifies the parameters of what is allowed. |
|  | Is there a new or significantly changed processing of PID or sensitive data? | E.g. use of external network storage | N |  |  |  |
|  | Will the processing result in a significant amount of new data being held? | Clear communications are needed to inform patient/staff | N |  |  |  |
|  | Will the processing result in the handling of new data about a significant number of people or a change in the population coverage? | Clear communications are needed to inform patient/staff | N |  |  |  |
|  | Will there be new or changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources? | Issues may arise in relation to data quality and accuracy. New data quality checks may need to be introduced | N |  |  |  |
|  | Does the processing involve new or changed data access, sharing, security or disclosure arrangements? |  | Y | Access controls will be in place - staff accessing the system will only be allowed access as befits their role.A new user form will have to be completed and authorised by a manager to allow access.System administrators will be responsible for adding and removing users from the system and maintaining a log of users. |  |  |
|  | Does the processing involve new or changed data retention arrangements? |  | Y | In line with Code of Practice Minor Record retention – 2 years only |  |  |
|  | Does the processing include public security measures or is exempted under law? | E.g. Crime, terrorism, public order and public health | N |  |  |  |

# Stage 2: Data Protection

To be completed with the Information Governance Team

| Question | Guidance | Your Response |
| --- | --- | --- |
| Who is Data Controller and Data Processor? |  | Data Controller – Maidstone and Tunbridge Wells NHS TrustData Processor – Service Works Group Ltd |
| Please list the ICO registration number for all organisation who will have access to the data | Gail, when I go onto the ICO website it asks for our registration number in order to search.. Can you advise please. | MTW - Z9042352Service Works Group Ltd |
| What IG contractual arrangements are in place? | IG clause for contract – Gail, please provide | NHS Standard Terms & Conditions |
| What personal data are you processing and for what purpose? | See definitions for PID in section 1.3. E.g. direct healthcare, employment of staff, audit or analysis. | Staff names – Estates Maintenance and Hotel Services – to allocate tasks.Patient names may occasionally be used when logging a portering job. |
| On what grounds are you legally processing personal data? | E.g. Consent (implied or explicit)Legal obligations e.g. public healthVital interests e.g. life or deathLegitimate interests of the data holder | Administration and management of healthcare services – the user is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller e.g., in order to provide healthcare services. |
| If explicit consent is required, how is it obtained and how will dissent to sharing be managed? |  | N/A |
| How do you inform individuals how their data is being used? | E.g. ICO registration & Fair Processing [patient advice] leaflets & posters. | N/A |
| If processing existing personal data for a new purpose, do you need to inform the individuals? |  | N/A |
| Is the new purpose compatible with the original purpose? | E.g. health records used to track missing persons. The purpose is not compatible. | Yes  |
| Can you confirm that anyone who will have access to the personal data is current with their annual mandatory IG training? | Link to IGTT | Yes – the user log will include a record of IG training dates |
| Have you checked the dataset is relevant, adequate & not excessive? | Refer to the Data Protection Principles & Caldicott Policy. | Yes |
| Do you check data for accuracy [numerical & free text]? |  | Yes – reports will be monitored |
| How long will the data be kept for and who is the information asset owner for the data set? |  | Maximum 2 years in line with Code of Practice Minor Record retentionInformation Asset Owner – Jeanette Batten |
| Describe your data loss contingency & back up plan. | Records may be paper, field based, mobile or network based, etc | Teams will revert to paper records, which will be entered onto the system once systems are back up and running. |
| Are you transferring data out of the UK? If so where? |  | No |
| Direct electronic marketing (text, email, phone, fax) must comply with the (PECR) Privacy & Electronic Communications Regulations 2003. |  | N/A |
| Statutory Compliance conclusion | (DPA, A2HRA, HRA etc). To be completed by the Information Governance Team | DPA 2018 compliant  |