**Data Flow Mapping**

|  |  |
| --- | --- |
| **Policy Group** | Information Governance |
| **Procedure No.** | 1 | **Version No.** | 1 |
| **Written by** |  | **Ratified By** |  |
| **Date Ratified** |  | **Review Date** |  |

This procedure is applicable to all staff working with ………[organisation name]…………..

**Purpose**

Data Flow Mapping will be undertaken in order for the organisation to understand and identify any person identifiable data (‘PID’) is being sent internally and externally throughout the organisation, how it is being sent and to capture any locally held PID.

This will enable the organisation to identify any security risks in the process used to send PID. Once identified the organisation will be able to assess the risk of any potential breach of confidentiality, reassess the processes used and thereby mitigate any identified risk.

Data Flow is the process by which information gets from one place to another and encompasses its final destination. Data Flow Mapping will ensure measures are in place to ensure data is filed, or reaches its destination, safely.

**Person Identifiable Data (‘PID’)**

This includes any data which contains a person’s name and/or other information which could identify the person to whom it relates. This may be information which stands alone or is read in conjunction with other data. A direct example would be a person’s name or a combination of Date of Birth and Postcode.

PID is applicable to both staff, clients, contractors, visitors.

**Information flows to be mapped**

Any type of exchange of PID should be mapped. Individual items do not need to be mapped. For example, ‘Letter to client’ would be a group and would be mapped rather than Letter to Mr B, Letter to Mrs C. Another example would be ‘Transporting data in the community’ rather than using an iPad when visiting ‘x’ venue and separately when visiting ‘y’ venue.

Mapping should include both inward and outward bound information.

Some examples are:

* A referral into the service
* Outcome letters sent to client, other third party or their GP
* Onward referral to another service
* Staff salaries
* Recruitment information
* Any web-based submission
* Automatic transfers from one information system to another organisation
* CQC correspondence and transfer of related evidence of procedures
* Use of the fax machine to send PID

**Internally held data to be mapped**

Mapping should include any physically held documentation.

Some examples are:

* Data held on spreadsheets or in databases which contain PID
* Records of help/advice/treatment given held in filing cabinets or archive boxes
* PID relating to service users or staff held on shared drives, local drives, flash drives, cloud, drop-box etc.
* Photographs and/or films of staff, service users or third party providers held by staff or centrally in the organisation
* Diaries, notebooks, telephone message books, use of ‘sticky notes’ if they contain PID
* Visitors sign-in books
* Confidential organisational data, eg financial
* Onward client information, eg transfers

The above examples are not exclusive.

Any method of storage or transfer of data which would be reported as an incident if lost should be included in Data Flow Mapping.

Telephone calls are not included as they are not a tangible method of transferring data. Recordings of any telephone calls should be included.

**Data Flow Mapping Spreadsheet**

Open the Data Flow Mapping Tool.

**Complete:**

Organisation Information – complete with name of organisation

Examples of Data – have a look and think about your own flow and types of data

Supporting Tab – ignore this, it has information to support drop down boxes in main document

Complete each row with a different type of data flow identified in your organisation

Send the completed spreadsheet to your Information Governance Officer/CEO

**Completed Data**

Your IG Officer/CEO will have a look at the completed data. It may be useful to meet with a small group to discuss ways some information could be transferred if the risk of a data breach appears high. It may be that a new process/procedure for transferring data is formulated and circulated to the team. This will help protect the organisation from litigation, reputational damage and any other resulting action from the potential loss of confidential data.

**Ongoing Actions**

It is important to update the Data Flow Mapping spreadsheet at least twice a year. It will also be updated should the organisation introduce a new method of transferring data containing PID.