Information Asset Risk Management Procedure v7

This procedure implements the Information Governance Policy providing information on Information Asset Risk Management and outlining the processes needed to ensure compliance with all legislative, regulatory and best practice requirements. It seeks to ensure the ethical, secure and confidential processing of information and use of information asset systems to support the provision of high-quality care.

BACKGROUND

Information risk is inherent in all administrative and business activities and everyone working for or on behalf of Young Epilepsy continuously manages information asset risk. This procedure recognises that the aim of information asset risk management is not to eliminate risk but, rather, to provide the structural means to identify, prioritise and manage the risks involved in all of Young Epilepsy's activities. It requires a balance between the cost of managing and treating Information asset risks with the anticipated benefits that will be derived.

This Information Asset Risk Procedure has been created to:

- Protect Young Epilepsy, its staff and its users from Information asset risks where the likelihood of occurrence and the consequences are significant;
- Provide a consistent risk management framework in which Information asset risks will be identified, considered and addressed in key approval, review and control processes;
- Encourage pro-active rather than re-active risk management;
- Provide assistance to and improve the quality of decision making throughout Young Epilepsy; and
- Assist in safeguarding Young Epilepsy's information assets.

In drafting this Procedure, the following legal and regulatory obligations and best practice guidance have been considered:

- Caldicott Principles;
- NHS Code of Practice on Confidentiality and Records Management;
- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018 (DPA 2018):
- NHS Records Management Code of Practice;
- Information Security Management;
- Information Governance Management;

- Information Quality Assurance (Data Accreditation);

Definitions

Risk

The chance of something happening, which will have an impact upon objectives. It is measured in terms of consequence and likelihood.

Consequence

The outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

Likelihood

A qualitative description or synonym for probability or frequency.

Risk Assessment

The overall process of risk analysis and risk evaluation.

Risk Management

The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.

Information Asset

An information asset is a body of information which has value to an organisation, for example care records in a filing cabinet, care records on planning software, employee training records. You should consider all personal data. You should record all information whether paper, CD, electronic, tape etc.

National Archive

An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles. Please refer to the Guide on Information Assets for more information on this Group.

Records

A record may be or may form part of an Information Asset. Please refer to the Guides on Records Management for more information, on records and how they should be managed.

Procedure format

1. Staff roles and responsibilities
2. Information Risk Management process
3. Strategies to reduce risk
4. Further guidance

1. Staff roles and responsibilities

All employees are responsible for information asset risk management to ensure the effective management of potential opportunities and risk. Responsibility specifically falls on the following members of Young Epilepsy's staff team with specific expertise and training in this area:

Accounting officer

Has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level (this role is undertaken by the Chief Executive)

Caldicott Guardian/Lead

Acts as the conscience of the organisation for patient information, patient confidentiality and information sharing issues and the proper management of patient information. *Please refer to separate Guide on this role for more information on this role.*

Data Protection Officer (DPO)

this role informs and advises the organisation on data protection obligations, monitors compliance with data protection laws and Young Epilepsy's own policies and is the first point of contact for supervisory authorities and for individuals. *Please refer to separate Guide on this role for more information on this role.*

Information Asset Owner (IAO)

The role of the Information Asset Owner is to understand and address risks to the information assets they 'own' and to provide assurance to the Senior Information Risk Owner (SIRO) on the security and use of those assets. *Please refer to separate Guide on this role for more information on this role.*

Information Asset Administrators (IAA)

Information Asset Administrators ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date. *Please refer to separate Guide on this role for more information on this role.*

Information Governance Steering Group (IGSG)

The IGSG is responsible for driving the overall promotion and implementation of Information Governance throughout Young Epilepsy. It must annually review and approve all IG related procedures. Please refer to the IGSG terms of reference for more information on this Group.

Senior Information Risk Owner (SIRO)

Is a member of the Executive team who is familiar with and takes ownership of the organisation's information risk and implementing the organisation's information risk strategy. *Please refer to separate Guide on this role for more information on this role.*

Responsibility for implementation

It is the responsibility of the staff listed below to ensure this policy and guidance are implemented effectively. This includes ensuring that records and documents are maintained for as long as is necessary, but no longer, in the context of Young Epilepsy's legal/regulatory obligations, operational business needs and the relevant retention schedule. These employees must also ensure that records and documents are properly disposed of

2. Information Risk Management process

Information Assets must be protected where the release or loss of data could cause:

- Harm or distress to patients or staff;
- Reputational damage
- Financial loss or exposure
- Major breakdown in information systems, information security or information integrity;
- Significant incidents of regulatory non-compliance

The following process must be followed:

a. Analyse the compliance

Before Information Assets are operational, their compliance with best practice and relevant governance standards, such as Data Protection, Confidentiality, Data Security Standards, Caldicott Principles etc. must be assessed and approved by an Exec Lead. This can involve completing the following documentation:

- IG compliance analysis
- Data Protection Impact Assessment
- Legitimate Interests Assessment
- Information Sharing Agreement.

Advice on what documentation is required and support on its completion can be obtained from the Data Protection Officer. *All of the above forms and guides can be found on the IG SharePoint page.*

b. Identify the Information Assets - Information Asset Register (IAR)

All IAOs and IAAs are responsible for identifying the information Assets they own or work with and for ensuring that these are recorded in the IAR. The Register is maintained on SharePoint and annually reviewed by the IGSG*. Guidance on this and the IAR can be found on the IG SharePoint site.*

c. Identify data flows and the lawful basis for these in the Record of Processing Activities (RoPA)

Each department should provide on the RoPA a broad outline of the data flows (incoming, outgoing and internal), method of transfer and lawful basis. *Guidance on this and the RoPA can be found on the IG SharePoint site.*

d. Assess the risks – risk assessment

Information Assets are assessed for risk using Young Epilepsy's Risk Assessment processes and methodology. The Data Protection Officer records the identified organisational risks on the IG risk register, which is reviewed by the IG Steering Group who may:-

- Accept the identified risks; or
- Review and re-assess the risks

IAOs or IAAs may record individual Information asset risks on their relevant departmental risk register. The IG Risk Register can be found on SharePoint.

e. Treat the risks

Risk treatment is the responsibility of all staff, who must select and implement the most appropriate options for dealing with risk. This may involve one or a combination of the following five strategies:

- Avoid the risk ;
- Reduce the likelihood of occurrence;
- Reduce the consequences of occurrence;
- Transfer the risk;
- Retain/accept the risk.

Issues may be referred to the IG Steering Group for consideration.

f. Monitor and review the information asset

IAOs and IAAs are responsible for monitoring and reviewing the risks that they have identified. This should be undertaken at least annually, but may also occur as specific issues arise.

Regular audits on data quality

3. Strategies to reduce risk

There are a number of strategies available to staff to reduce the risk associated with their Information Asset. The IG Steering Group, Data Protection Officer and Senior Information Risk Owner can advise on which of the following options is most suitable and the best technique to employ.

Separate Guides on each of the following strategies listed below are available on the IG SharePoint page.

a. Anonymisation

Anonymised information is information that does not identify an individual directly or indirectly. Once information is anonymised it ceases to be both personal data and confidential information.

b. Business data and cyber continuity plans

The need to assess and maintain continuity plans, now sits within the Major Incident Management team, and is led by the Exec team.

c. Computer based information assets

Access controls and related functionality are used to reduce the risks associated with information assets. All computer-based information assets must have a system level security policy, containing rules regarding its access controls. Multi factor authentication should be activated wherever possible. Any queries should be referred to the Head of IT Services.

c. Encryption

Encryption, to the level approved by Young Epilepsy, will reduce the risk of unauthorised access to information. All laptops, USB sticks or other mobile media that carry personal data or sensitive organisational information must be encrypted by the IT department prior to use.

d. Homeworking

It is important to manage and prevent unacceptable risks both to Young Epilepsy and other information assets through the use of unapproved or unsafe home working facilities. All homeworkers must ensure that they meet the necessary standards, outlined in Guidance. To take records off campus the 'Taking records off campus form' must be completed and authorised by the relevant Exec Lead. Any queries should be referred to the relevant Head of Department or member of the Exec Team or the DPO.

e. Pseudonymisation

Pseudonymisation is a technique whereby the information shared is anonymous to the recipient, because identifiers such as name, NHS number etc, have been removed and are then replaced with a number or letter. This means that the data remains identifiable to the sender should the recipient raise a query about some of the data shared.

f. Redaction

Removing all personal data from a document would prevent an IG breach, if it disclosed inappropriately or outside of the organisation. However, it is recognised that this is will not always be a suitable method of risk reduction where the personal data is essential to the integrity of the record, in such cases another method such as risk reduction strategy may be more suitable.

g. Secure destruction

Young Epilepsy has a duty to ensure that all records, both digital and hard copy, it destroys are destroyed in a secure manner. The options available have been identified and must be implemented by all staff.

h. Sharing information securely

There are a number of methods, (email, Office 365, post, courier etc.) by which information can be transferred. These have been assessed for risks and strategies to reduce these have been identified by Young Epilepsy and must be implemented by staff.

i. Staff training

All staff must complete Information Governance training, and pass a test on this, as part of their induction programme. All staff must also annually complete IG training, as part of the Data Security & Protection Toolkit. Additional training will also be provided for specific roles, such as the SIRO and DPO.

j. Using NHS numbers

The NHS Number is the only national unique patient identifier in operation in the NHS. Using the NHS Number makes it possible to share patient information safely, efficiently and accurately across NHS and partner organisations

All Young Epilepsy student records that may go outside of the organisation and all digital records must include the student's NHS number. It must also be used on the records of any other service user who receives medical or healthcare provision from Young Epilepsy.

k. Data collection & validation activities

All those involved in the care of an individual need to be able to rely on the accuracy of the available information in order to be able to provide timely and effective treatment or care for that individual.

To maintain the integrity of service user information and to minimise risk, Young Epilepsy has procedures in place for the collection of service user information and for checking the information held on all systems and/or in records that support the provision of care with the source. These include

- Documenting procedures for collecting and recording information – this must be undertaken by all directorates, who should annually review these and provide copies to HR;
- Auditing access to Information asset - the Head of IT Services must produce an annual report for the IG Steering Group;
- Establishing and maintaining procedures for tracking files - all department heads must establish and maintain procedures to ensure that the new location of a record is noted whenever it is removed from its usual location;
- Validation of records – all Heads of Department must annually validate the departmental records with regard to:
  - ~ Record keeping standards;
  - ~ Accuracy of hard copy and electronic records.

  A member of the staff team who is not usually responsible for data entry should undertake the validation

  An annual report of the validation and issues identified should be made to the Information Governance Steering Group by March of each year

D. Further guidance

- ### Information Risk Management guides

  This procedure is supported by a number of specific data protection guides, which are available to all staff on the IG SharePoint page.

  Information Governance - Information Risk Management Guides (sharepoint.com)

- ### Other Guides

  As there is some overlap between many of the information-related procedures, additional information may also be found in the Confidentiality, Data Protection, and Information Governance procedures and Guides available to all on SharePoint.

  Information Governance - IG Policies, Procedures and Guides (sharepoint.com)

- ### Guidance and advice

If further detail, guidance, or advice is needed, please do not hesitate to use the following contact details

~	Person:	Susan Turner, Data Protection Officer (DPO) & IG Manager;
~	Telephone:	Ext. 286;
~	Email	sturner@youngepilepsy.org.uk