Information Governance Procedure

This procedure implements the Young Epilepsy/St Piers' Information Governance Policy providing further information on Information Governance 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 systems to support the provision of high quality care.

BACKGROUND

This procedure details the management structure and responsibilities that are in place for effective and compliant information governance. It establishes and promotes a culture of good practice around the processing of information and use of information systems that supports the provision of high-quality care to our students and other service users.

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

- Caldicott Principles;
- The Confidentiality NHS Code of Practice;
- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018 (DPA 2018);
- Records Management NHS Code of Practice;
- Privacy and Electronic Communication Regulations;
- Information Security Management;
- Information Governance Management;
- Information Quality Assurance (Data Accreditation).

Definitions

NHS Connecting for Health defines Information Governance as:

> "*the structures, policies and practice of the healthcare industry, the DH, the NHS, the Independent sector and its suppliers to ensure the confidentiality and security of all records, and especially patient records, and to enable the ethical use of them for the benefit of individual patients and the public good.*
>
> *IG is a series of best practice guidelines and principles of the law to be followed by NHS/Social Care organisations and individuals. IG is the core foundation for high quality healthcare using good quality information.*
>
> *Good Information Governance practice ensures necessary safeguards for, and appropriate use of corporate, patient and personal information."*

The Department of Health, Information for Social Care, defines Information Governance as having the following aims:

- *To support the provision of high quality care by promoting the effective and appropriate use of information.*
- *To encourage responsible staff to work closely together, preventing duplication of effort and enabling more efficient use of resources.*
- *To develop support arrangements and provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards.*
- *To enable organisations to understand their own performance and manage improvement in a systematic and effective way.*

Responsibilities

Senior Information Risk Owner (SIRO)

The SIRO is a member of the Exec team, who is responsible for overseeing Information Governance (IG) risk and implementing the organisation's information risk strategy.

Data Protection Officer/Information Governance Manager

The IG Lead is responsible for ensuring effective management, accountability. Compliance and assurance in IG issues.

The Information Governance Steering Group (IGSG)

The IGSG is responsible for driving the overall promotion and implementation of IG throughout Young Epilepsy/St Piers. It must annually review and approve all IG related procedures.

The IGSG will report on the management of the information risks in statements of internal controls and to include details of data loss and confidentiality breach incidents in an annual report to the Executive team.

All staff

All employees are responsible for identifying new processes and information assets that might impact on information security, confidentiality, data protection and information quality.

Procedure format

A. Data Security & Protection Toolkit
B. The Caldicott Principles
C. IG Compliance Analysis
D. IG Incidents
E. Records management
F. Sharing information

G. IG training
H. Information Security
I. IG Framework
J. Further guidance

A. Data Security & Protection Toolkit (DSPT)

Young Epilepsy/St Piers is committed to meeting the standards required of NHS Business Partners, as contained in the DSPT. This includes the review of existing policies, procedures and guides and where necessary the development of new guidance to ensure compliance with the DSPT. This is an annual process undertaken by the IG Lead with support from the IG Steering Group.

Data Security Standards

The DSPT is based on the National Data Guardian's Data Security Standards. Young Epilepsy/St Piers and its staff must therefore apply the following standards at all times:-

DSS 1 'All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.'

DSS 2 'All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.'

DSS 3 'All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.'

DSS 4 'Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.'

DSS 5 'Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.'

DSS 6 'Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.'

DSS 7 'A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.'

DSS 8 'No unsupported operating systems, software or internet browsers are used within the IT estate.'

DSS 9 ‘A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.’

DSS 10 ‘IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian’s Data Security Standards.’

B. The Caldicott Principles

Young Epilepsy/St Piers and its staff are committed to applying the eight Caldicott Principles to health and social data at all times: -

1. Justify the purpose (s) for using confidential information;
2. Only use it when absolutely necessary;
3. Use the minimum that is required;
4. Access should be on a strict need-to-know basis;
5. Everyone must understand his or her responsibilities;
6. Understand and comply with the law;
7. The duty to share information can be as important as the duty to protect confidentiality. (This Principle must not be applied without having consulted with the Data Protection Officer first.)
8. Inform patients and service users about how their confidential information is used

C. IG Compliance Analysis processes

Staff must follow the IG Compliance Analysis process for all information assets and processing that they are responsible for. The following forms and records are used in order to ensure that processing complies with the UK GDPR, DPA 2018 , Privacy and Electronic Communication Regulations, DSPT, Information Commissioner’s Office guidance and other relevant guidance/standards.

- Annual Renewal of information asset.
- Data Protection Impact Assessment (DPIA) forms
  - Screening form
  - Routine
  - Extended
  - Health and social care data;
- IG Compliance Analysis form;
- Information Asset Register;
- Legitimate Interests Assessment
- Privacy & Electronic Communications Regulation form;
- Summary of Processing form;

Where the processing is taking place on an information society services, such as a website or platform, that may be accessed by young people, the following documentation should also be completed:

- Age Appropriate Design Code DPIA.

D. IG Incidents and breaches

An IG incident is any unusual problem, occurrence, or other situation that is likely to lead to undesirable effects or that is not in accordance with established policies, procedures or practices. It includes near misses and unsafe processes.

An IG incident is an event, or chain of events, that could compromise the information's:-

a. Confidentiality;
b. Integrity; and/or
c. Availability.

An IG incident is not necessarily a data breach.

Reporting responsibilities

All incidents and breaches must be reported as soon as an individual has identified or is concerned that an incident has taken place.

All staff must report incidents to the Data Protection Officer (DPO) and, if IT related, to the Head of IT, using the IG Incident Reporting form. Incidents will be investigated and recommended action identified, as part of the lessons learned process.

The DPO and Senior Information Risk Owner, in consultation with the Chief Executive Officer, are responsible for determining whether an incident is notifiable and if it is they are responsible for reporting it using the DSPT Reporting Tool.

IG Incident records

The DPO and Head of IT must keep a record of all IG Incidents. A summary of incidents must be provided at each IGSG meeting and be included in the DPO's report to the Trust Board.

E. Records Management

Responsibility

Young Epilepsy/St Piers' procedures and guides establish and maintain the processes for the effective management of records. These are outlined in the Records Management Guidance and Roadmap.

Managers must ensure effective records management within their areas. Staff are responsible for ensuring that they adhere to Young Epilepsy/St Piers' records management standards.

Records management is promoted through:

- Policies and procedures;
- Raising Awareness;
- Training;

All Heads of Departments must undertake annual assessments and audits of their department's records management.

Archive Records

Young Epilepsy/St Piers keeps archive records, in accordance with the organisation's retention schedules.

Records Format

To ensure that all records are organised and referenced in the same way, staff must adopt the standard formats agreed by Young Epilepsy/St Piers.

F. Sharing Information

Personal and special category personal data may only be shared if a lawful basis has been identified in the UK GDPR /DPA 2018.

Confidential information may only be shared if there is a legal basis for doing so (as outlined in the Confidentiality Procedure and related guides).

Seeking consent

It is Young Epilepsy/St Piers' policy that whenever possible and appropriate consent should be obtained. This may be obtained through the use of the relevant Privacy notice, standard data protection consent forms or ad hoc issue specific forms.

The seven golden rules of information sharing

1. Remember that the UK GDPR , DPA 2018 and human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.
2. Be open and honest with the student/parent/staff/service user from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
3. Seek advice from the IG Lead, if you are in any doubt about sharing the information concerned, if possible, without disclosing the identity of the individual concerned.
4. Where possible, share information with consent and respect the wishes of those who do not consent to having their information shared. Under the UK GDPR and DPA 2018 you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk - this will require you to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear of the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared.

5. Consider safety and well-being: base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.
6. Necessary, proportionate, relevant, adequate, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles).
7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

G. IG Training

All staff

All Young Epilepsy/St Piers staff must complete Young Epilepsy/St Piers' own Information Governance training and achieve a pass rate in the quiz completed at the end of the training session. Staff must also annually complete an e-learning module, as required by the DSPT.

Additional training

The Learning and Development department or the Information Governance Manager may additionally identify additional information Governance training for individuals or staff roles.

H. Information Security

Young Epilepsy/St Piers promotes confidentiality and security practice to its staff through it policies, procedures and guides as well as training and awareness raising activities.

All Young Epilepsy/St Piers staff must:

- Establish and maintain policies for the effective and secure management of its information assets and resources;
- Undertake risk assessments to ensure that appropriate security controls are in place for existing or potential information systems.

I. Information Governance Framework

Information Governance is a framework that enables Young Epilepsy/St Piers to:

- Establish a good practice around the handling of information
- Promote a culture of awareness and improvement
- Comply with legislation and other mandatory standards

It comprises the following areas:

- Confidentiality and data protection assurance
- Legal compliance
- Information security
- Information quality assurance

J. Further guidance

- Information Governance guides

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

  Information Governance - Information Governance 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 Risk Management 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