Please note our disclaimer:
https://www.careprovideralliance.org.uk/disclaimer.html

An Introduction to Information Governance for Registered Managers

A. What is Information Governance?

Information Governance (IG) is the way in which organisations safeguard people's personal information. This includes knowing when it is appropriate to share information, not just keeping information secure, protected and safe.

IG involves people, processes and technology to ensure the safety and effectiveness of information sharing.

People - this means knowing who is responsible for information security

Process - this can include policies, procedures, processes and controls

Technology - anything from using paper systems to completely paperless ways of working.

IG specifically covers personal information (e.g. service users and employees) and corporate information (e.g. financial records). This covers all forms of information whether it is stored on paper, on computers, or is verbal information.

B. Why is it important?

Service users and staff trust care providers to keep their personal information safe.

Staff have a duty to treat personal information confidentially; for social care staff, this duty is set out in the Skills for Care Code of Conduct. However, staff also have a duty to share information and it is important that this is done in line with regulations.

The Department of Health and Social Care have provided Data Security and Protection guidance on the steps that health and care organisations should take to comply with the 10 data security standards [see D].

The safeguarding of confidential and sensitive information is a legal and regulatory requirement. There are many rules which surround information handling e.g.

i. The **Care Quality Commission (CQC)** - Several Key Lines of Enquiry (KLOEs) now link to IG. For example, Well-Led 2.8 and 5.2. You must comply with the CQC KLOEs as a minimum registration requirement.

ii. The **General Data Protection Regulation** (GDPR) and **Data Protection Act 2018** (DPA) replaced the existing Data Protection Act (1998) from 25th May 2018. This is a significant change to data protection law. The Information Commissioner's Office (ICO) is the regulatory body which enforces compliance with the GDPR/DPA. **Every Care Provider is required to register with the ICO.**

iii. **NHS Standard Contracts** with local NHS bodies – For social care providers who provide care through the NHS Standard Contract, it will be mandatory to comply with the Data Security & Protection Toolkit from April 2018. It is recommended but not mandatory for providers who do not provide care through the NHS Standard Contract to help demonstrate compliance against the 10 data security standards [see below] and GDPR/DPA.

iv. **10 Data Security Standards** – These were proposed by the National Data Guardian and accepted by the Government last year.

C. What is the Data Security and Protection Toolkit?

The Data Security & Protection Toolkit is available for submissions for the 2018/2019 financial year. It is an online tool that allows organisations to measure their performance against the 10 data security standards. The Toolkit has been tested with the social care sector and designed with care providers in mind.

The Toolkit is self-assessed; this means that it is your responsibility to review your organisation's current policies and procedures to see if any changes will need to be made to meet the requirements. If you are compliant with the Toolkit, this is considered evidence that you have good IG practices in place. The Toolkit is also a valuable framework for demonstrating your compliance with data protection legislation.

Although CQC **do not** assess submissions to the Toolkit, working through this will provide you with ample evidence that you have IG policies and procedures in place to satisfy their requirements.

As well as being a useful tool for self-assessing your IG compliance, successful Toolkit submissions are the first step in gaining access to national systems including:

i. NHSmail (https://portal.nhs.net/Help/joiningnhsmail)

ii. Summary Care Record - Work has started to investigate the best secure way for care providers to access the SCR, which contains key information from General Practitioners including medication, allergies and adverse reactions.

A full list of potential services is available here:
https://digital.nhs.uk/article/200/Community-and-Social-care

D. Information Sharing and Consent

Citizen consent is a fundamental of the Health and Social Care system. This applies not only to the care that they receive but is also true for the information that we keep and share. It is important that our service users know and understand how their information is being stored and used and who has access to it.

All citizens have the right to be involved in the preparation, review and continued management of their care plans and should know how their records will be made available to them.

Information should only be shared when there is a justified reason to do so and/or with the consent of the service user. The Caldicott Principles [below] provide guidelines for the safe and proper sharing of information within the Health and Social Care sector.

i. Justify the purpose(s).

ii. Don't use personal confidential data unless it is absolutely necessary.

iii. Use the minimum necessary personal confidential data.

iv. Access to personal confidential data should be on a strict need-to-know basis.

v. Everyone with access to personal confidential data should be aware of their responsibilities.

vi. Comply with the law.

vii. The duty to share information can be as important as the duty to protect patient confidentiality.

Information Governance is concerned with ensuring that personal and sensitive information is kept safe.

It is not intended to be a barrier to sharing appropriate information.

E. What should I do now?

The Department of Health and Social Care has produced the following guidance: https://www.gov.uk/government/publications/data-security-and-protection-for-health-and-care-organisations

As you begin to work on IG you should consider the following:

People

1. Who is going to lead on IG/data security? This could be the Registered Manager, a deputy or other senior person in a champion role. They will implement and audit IG within your organisation. The lead has 2 key responsibilities:
    a. Responsibility for managing information risk
    b. Responsibility for protecting service user rights

2. As part of your annual mandatory training all staff should be trained on IG. To start, all staff should have read and understood the accompanying guidance '*An Introduction to Information Sharing for Staff*'. There is free e-learning available on Data Awareness.

Process

1. The lead will need to review your organisation's policies and procedures and any internal audits that need to be completed. Material is available on the Care Provider Alliance website to assist with this.

2. A good starting point is to assess what information your organisation holds and shares.

Technology

1. Technology needs to be used appropriately to support your service while understanding that much of the information stored may be confidential. You should take appropriate steps to protect whatever technology is deployed within your organisation.

2. If you use computers in your organisation, it is vital that you are aware of the need to ensure Cyber Security. All staff should read 'An Introduction to Cyber Security'.

Please note our disclaimer:
https://www.careprovideralliance.org.uk/disclaimer.html

F. Resources and further support

Name	Type of Support	Contact Details
Care Quality Commission	Regulatory guidance.	http://www.cqc.org.uk/guidance-providers
Care Provider Alliance	Templates and guidance materials for DSP Toolkit and Cyber Security.	https://www.careprovideralliance.org.uk/information-governance.html
Skills for Care	Guidance on securely sharing information. Advice on training and digital skills.	http://www.skillsforcare.org.uk/Topics/Digital-skills/Digital-working.aspx
Information Commissioner's Office	Guidance on the Data Protection Act and the General Data Protection Regulation.	www.ico.org.uk
Information Governance Alliance	Guidance on using and sharing information in the Health and Care sectors and GDPR.	https://digital.nhs.uk/information-governance-alliance
NHS Digital	General guidance and technical support on the Toolkit and on cyber security.	https://digital.nhs.uk/home https://digital.nhs.uk/cyber-security
National Data Guardian (Dame Fiona Caldicott)	The 10 Data Security Standards	https://www.gov.uk/government/organisations/national-data-guardian
Cyber Aware	Information about Cyber Security.	https://www.cyberaware.gov.uk/
Get Safe Online	A public & private sector partnership providing practical advice on how to protect yourself from online threats.	https://www.getsafeonline.org
National Cyber Security Centre	UK Authority on Cyber Security.	https://www.ncsc.gov.uk/

G. 10 Data Security Standards

People: ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.	**Process:** ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.	**Technology:** ensure technology is secure and up-to-date.
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	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.	8. No unsupported operating systems, software or internet browsers are used within the IT estate.
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.	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.	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.
3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.	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.	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.
	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.	