

# An Introduction to Information Governance for Registered Managers

## 1. What is Information Governance?

Information Governance 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 safe.

Information Governance 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 paperless ways of working

Information Governance 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.

## 2. Why is it important?

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

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 safeguarding of confidential and sensitive information is a legal and regulatory requirement. There are many rules which surround the handling of information  
*For Example*

1. The [Care Quality Commission \(CQC\)](#) will be inspecting arrangements for information sharing from October 2017. In 4 out of the 5 categories there are Key Lines of Enquiry (KLOEs) for which Information Governance is directly relevant. You must comply with the CQC KLOEs as a minimum registration requirement.

2. **The Data Protection Act 1998** sets out the [Data Protection Principles](#). The General Data Protection Regulation (GDPR) will be coming into force from May 2018; this will supersede the Data Protection Act.
3. **NHS Contracts** with local NHS bodies – you may well have been asked to sign a contract with your CCG or Local Authority which asks that you comply with Information Governance requirements. This may include specifying compliance with the Information Governance (IG) Toolkit [see below].

The Information Commissioner's Office (ICO) is the regulatory body which enforces compliance with the Data Protection Act 1998.

**It is a requirement that every Care Provider registers with the ICO.**

### 3. How do I become compliant?

The rest of this guidance is designed to help you to be compliant with Information Governance regulations – by supplying:

- Policies
- Exemplary material; and
- Training tools on Information Governance for staff.

The materials are available free of copyright, so they can be used and adapted by any person or organisation. The general approach is to use the Information Governance (IG) Toolkit to self-assess your compliance and subsequently develop an improvement plan to implement over the rest of the year.

**All Care Providers are expected to complete the IG Toolkit as the Department of Health has stated that all organisations which have access to NHS patient data must evidence their Information Governance compliance in this way.**

### 4. What is the Information Governance Toolkit?

The [IG Toolkit](#) has been designed by the Department of Health (DH) and NHS Digital. It pulls together all guidance into a standard set of requirements which cover all applicable regulatory matters.

The IG 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 in order to meet the requirements. If you are compliant with the IG Toolkit,

this is considered evidence that you have good Information Governance practices in place.

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

## 5. 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. This may be covered in your General Consent on Admission Form or similar.

All citizens have the right to be involved in the preparation, review and continued management of their care plans and should know how their health 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.

**Principle 1:** Justify the purpose(s).

**Principle 2:** Don't use personal confidential data unless it is absolutely necessary.

**Principle 3:** Use the minimum necessary personal confidential data.

**Principle 4:** Access to personal confidential data should be on a strict need-to-know basis.

**Principle 5:** Everyone with access to personal confidential data should be aware of their responsibilities.

**Principle 6:** Comply with the law.

**Principle 7:** 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.**

## 6. First Steps:

As you begin to work on your Information Governance you should consider:

### People

1. Who is going to be the Information Governance (IG) Lead? *i.e.* the person responsible for Information Governance - this could be the Registered Manager, a deputy or other senior person. They will implement and audit Information Governance within your organisation. The IG Lead has 2 key responsibilities:
  - a. Responsibility for managing information risk
  - b. Responsibility for protecting service user rights
2. The IG Lead will need to determine what level of training they personally require, and what training will be appropriate for the rest of the staff. This IG training should form part of your organisation's annual mandatory training. As a minimum, all staff should have read and understood the '*Introduction to Information Governance for Staff*'.

### Process

1. The IG Lead will need to review your organisation's policies and procedures and any internal audits that need to be completed. These policies and procedures may need enhancement to reflect legislative changes. The rest of this guidance is designed to facilitate this audit and enhancement process by providing a range of guidance and exemplars for use and adaption.

### 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 any computers in your organisation, it is vital that you are aware of the need to ensure [Cyber Security](#).

## 7. Ensuring ongoing Information Governance Compliance

It is important to make sure that you stay up to date.

In page 4 of the *How-To Guide* there are questions for your IG Lead to work through so that they can develop a robust plan for ensuring compliance in the future.

## 8. Resources and further support

Name	Type of Support	Contact Details
Care Quality Commission	<ul style="list-style-type: none"> <li>Policy Statement: Information Security &amp; Governance</li> </ul>	<ul style="list-style-type: none"> <li><a href="https://goo.gl/hvvj5N">https://goo.gl/hvvj5N</a></li> <li><a href="http://www.cqc.org.uk/guidance-providers">http://www.cqc.org.uk/guidance-providers</a></li> </ul>
Skills for Care	<ul style="list-style-type: none"> <li>Guidance on securely sharing information.</li> </ul>	<ul style="list-style-type: none"> <li><a href="http://www.skillsforcare.org.uk/Documents/Topics/Digital-working/Information-sharing-for-social-care-employers.pdf">http://www.skillsforcare.org.uk/Documents/Topics/Digital-working/Information-sharing-for-social-care-employers.pdf</a></li> </ul>
Information Commissioner's Office	<ul style="list-style-type: none"> <li>Guidance on the Data Protection Act and the General Data Protection Regulation.</li> <li>Help with Registration.</li> </ul>	<ul style="list-style-type: none"> <li>0303 123 1113</li> <li><a href="http://www.ico.org.uk">www.ico.org.uk</a></li> <li><a href="mailto:registration@ico.org.uk">registration@ico.org.uk</a></li> </ul>
Information Governance Alliance	<ul style="list-style-type: none"> <li>Guidance on rules on using and sharing information in the Health and Care sectors.</li> </ul>	<ul style="list-style-type: none"> <li><a href="https://digital.nhs.uk/information-governance-alliance">https://digital.nhs.uk/information-governance-alliance</a></li> </ul>
NHS Digital	<ul style="list-style-type: none"> <li>General guidance and technical support on the IG Toolkit and on Cyber Security.</li> </ul>	<ul style="list-style-type: none"> <li>0300 3034034</li> <li><a href="https://www.digital.nhs.uk/article/364/Information-security-and-standards">https://www.digital.nhs.uk/article/364/Information-security-and-standards</a></li> <li><a href="mailto:enquiries@nhsdigital.nhs.uk">enquiries@nhsdigital.nhs.uk</a></li> </ul>
National Data Guardian (Dame Fiona Caldicott)	<ul style="list-style-type: none"> <li>"The National Data Guardian advises and challenges the health and care system to help ensure that citizens' confidential information is safeguarded securely and used properly."</li> </ul>	<ul style="list-style-type: none"> <li><a href="https://www.gov.uk/government/news/government-responds-on-cyber-security-and-data">https://www.gov.uk/government/news/government-responds-on-cyber-security-and-data</a></li> <li><a href="https://www.gov.uk/government/organisations/national-data-guardian">https://www.gov.uk/government/organisations/national-data-guardian</a></li> </ul>
Cyber Aware	<ul style="list-style-type: none"> <li>Information about Cyber Security.</li> </ul>	<ul style="list-style-type: none"> <li><a href="https://www.cyberaware.gov.uk/">https://www.cyberaware.gov.uk/</a></li> </ul>
Get Safe Online	<ul style="list-style-type: none"> <li>A public &amp; private sector partnership providing practical advice on how to protect yourself from online threats.</li> </ul>	<ul style="list-style-type: none"> <li><a href="https://www.getsafeonline.org">https://www.getsafeonline.org</a></li> </ul>
National Cyber Security Centre	<ul style="list-style-type: none"> <li>UK Authority on Cyber Security.</li> </ul>	<ul style="list-style-type: none"> <li><a href="http://www.ncsc.gov.uk/">www.ncsc.gov.uk/</a></li> </ul>