Job Description

Job Title:	Information Governance Officer
Reports to (job title):	Senior Information Governance Officer
Line Manager to:	N/A

Job purpose

The Information Governance Officer will be responsible for the management of the Information Governance Agenda across HCRG Care Group Services. Supporting the day-to-day operational delivery of Information Governance and ensuring that standards are commensurate of those set out within the Data Security & Protection Toolkit and comply with UK Data Protection laws.

Base

The role will be predominantly based at home with a requirement to travel to the services a few times a year.

This post is responsible for

- Promoting good IG practices which are aligned to the Data Security and Protection Toolkit (DSPT), the ICO Accountability Framework (AF), UK Data Protection laws and other areas within the IG Framework.

Key responsibilities

This list is intended to summarise the key responsibilities and is not intended to cover every task that may be required of the role.

- To provide day to day management of IG Projects as assigned by the Senior IG Officers and Head of IG.
- Provide timely advice and guidance to colleagues that aligns to IG policies and procedures and supports the business strategy
- Be a positive ambassador for Information Governance and promote awareness and best practice to internal and external stakeholders of all levels;
- Consider data protection by design and default for the efficient management and effective use of information and knowledge assets, in line with legal requirements and NHS initiatives.
- To proactively support the IG Team with the management of the CAF aligned Data Security and Protection Toolkit, Information Governance framework and annual work programmes to ensure consistency of approach and good practice across the organisation.
- Act as person responsible for obtaining, collating and providing relevant evidence for the CAF aligned Data Security and Protection Toolkit (DSPT) as delegated by the Head of IG.

- Proactively manage information incidents raised by colleagues through the incident reporting system, providing prompt mitigation advice, identifying trends and weaknesses in processes so improvements can be made. Where necessary provide incident response training or organisation learning sessions;
- Ensure that any potentially reportable incidents or are escalated to the Data Protection Officer and Business Unit senior leadership team in a timely manner and monitor compliance with reporting timescales;
- Maintain and promptly update KPI's, risks and other activity that falls within the IG Framework;
- Actively engage with the Business Units and services to identify projects and initiatives that may require data protection input;
- Provide efficient IG support and guidance to projects to ensure all activities are developed with data protection by design and default. This will include supporting the completion of data protection impact assessments, maintaining records of data processing activities, data processor due diligence and updating business unit and services privacy notices;
- Support mobilisations and exits where directed, following the project plan to ensure Information Governance practices are followed;
- Offer Data protection and Information Governance training and provide necessary support and guidance to staff. Actively promote the quality and safety training in IG to motivate colleagues to achieve the 95% annual compliance target.
- Attend Service and IG related meetings where required, internal and externally fostering positive relationships with all stakeholders.
- Maintain an awareness of all aspects of legislation, national guidance and policy relating to Information Governance and specifically the new data protection laws.
- Review and update national IG Policies to ensure they remain up to date.
- Monitor IG compliance across the organisation through audits and provide feedback and recommendations for improvements
- Support the collation and review of Information Assets and liaise with Records Manager to ensure that ROPAs and Information Assets are updated within agreed timeframes.

Our values

Our values are our moral compass and core to our DNA. They underpin the way we deliver our services and treat those who use our services.

To many organisations values are just words which don't translate into reality of the day to day but our values flow through everything that we do, they define who we are, what we stand for and set the expectations of our colleagues, communities, customers and partners. They have been defined by our colleagues and have been integral to our journey so far and will be integral to our future as well.

We have three values which help us stand out from the crowd, not just because there's only three, but because they are unique to who we are. We care, we think, and we do.

Job Description

Care	Think	Do
• Inspire	• Challenge	• Accountability
• Understand	• Improve	• Involve
• Communicate	• Learn	• Resilience

Confidentiality and Information Security

As our employee you will be required to uphold the confidentiality of all records held by the company, whether patients/service records or corporate information. This duty lasts indefinitely and will continue after you leave the company's employment.

All information which identifies living individuals in whatever form (paper/pictures, electronic data/images or voice) is covered by the 2018 Data Protection Act and should be managed in accordance with this legislation. This and all other information must be held in line with NHS national standards including the Records Management: NHS Code of Practice , NHS Constitution and HSCIC Code of Practice on Confidential Information and should only be accessed or disclosed lawfully. Monitoring of compliance will be undertaken by the Company. Failure to adhere to Information Governance policies and procedures may result in disciplinary action and, where applicable, criminal prosecution.

Information governance responsibilities

You are responsible for the following key aspects of Information Governance (not an exhaustive list):

- Completion of annual information governance training
- Reading applicable policies and procedures
- Understanding key responsibilities outlined in the Information Governance acceptable usage policies and procedures including NHS mandated encryption requirements
- Ensuring the security and confidentiality of all records and personal Information Assets
- Maintaining timely and accurate record keeping and where appropriate, in accordance with professional guidelines
- Only using email accounts authorised by us. These should be used in accordance with the Sending and Transferring Information Securely Procedures and Acceptable Use Policies.
- Reporting information governance incidents and near misses on CIRIS or to the appropriate person e.g. line manager, Head of Information Governance, Information Security Lead
- Adherence to the clear desk/screen policy
- Only using approved equipment for conducting work business

Job Description

Governance

Clinical governance is a framework through which organisations delivering health and care services are accountable to continuously improving the quality of their services and safeguarding high standards of care by creating an environment in which clinical and other forms of care flourishes. Employees must be aware that clinical governance places a duty on all staff to ensure that the level of care services they deliver to patients is safe and high quality, and that they follow/comply with our policies and procedures.

Registered Health Professional

All staff who are a member of a professional body must comply with standards of professional practice/conduct. It is the post holder's responsibility to ensure they are both familiar with and adhere to these requirements.

Risk Management/Health & Safety

The post holder has a responsibility to themselves and others in relation to managing risk, health and safety and will be required to work within the policies and procedures laid down by the company. Staff are required to observe the Hygiene Code and demonstrate good infection control and hand hygiene.

Employees must be aware of the responsibilities placed on them by the Health & Safety at Work Act (1974) to ensure that the agreed safety procedures are carried out to maintain a safe environment for other employees, patients and visitors. It is essential to observe strict fire and security precautions at all times.

All staff must report accidents, incidents and near misses so that the company can learn from them and improve safety.

Safeguarding Children and Vulnerable Adults Responsibility

We are committed to safeguarding and promoting the welfare of children and adults at risk of harm and expects all employees to share this commitment.

Medicines Management Responsibility

Nursing or registered healthcare professionals

Undertake all aspects of medicines management related activities in accordance within the company's medicines policies to ensure the safe, legal and appropriate use of medicines.

Skilled non-registered staff

Undertake all aspects of medicines management related activities in accordance with the company's medicines policy where appropriate training has been given and competencies have been achieved.

Job Description

Policies and Procedures

All colleagues must comply with the Company Policies and Procedures which can be found on the company intranet.

General

We are committed to serving our community. We aim to make our services exemplary in both clinical and operational aspects. We will show leadership in identifying healthcare needs to which we can respond and in determining the most cost-effective way of doing so.

We recruit competent staff that we support in maintaining and extending their skills in accordance with the needs of the people we serve. We will recognise the commitment from our staff to meeting the needs of our patients.

The company recognises a "non-smoking" policy. Employees are not able to smoke anywhere within the premises or when outside on official business.

Equal Opportunities

It is the company's intention to be an employer of choice and ensure that no job applicants or employees are unfairly disadvantaged on the grounds of gender, disability, race, ethnic origin, colour, age, sexual orientation, religion or belief, trade union membership or any other factors that are not relevant to their capability or potential. To this end, the company has an Equality and Diversity policy and it is the responsibility of each employee to contribute to its success.

Flexibility Statement

This job description is not exhaustive and may change as the post develops or changes to align with service needs. Any such changes will be discussed directly between the post holder and their line manager.

Job Description

Personal Specification

Essential

- BCS Data Protection Qualification, CIPPE, Certified GDPR/DPA Training, Information Governance Certificate for Health & Social Care or equivalent qualification or IG experience within a health and social care environment.
- A minimum of 1-2 years' experience working in the field of Information Governance, developing information sharing agreements, carrying out Data Protection Impact Assessments and documenting Records of Processing Activities
- A comprehensive understanding of regulatory compliance and risk associated to Data Protection and information security.
- Experience managing internal data protection and information security audits and training programs and overseeing the process of compliance with cyclical audits and reviews
- Strong influencing skills;
- Strong communication, both written and verbal, being highly personable with ability to network with a range of stakeholders and become a trusted business advisor;
- Ability to work both at a strategic level and be analytical and detail oriented as the appropriate activity requires;
- Experience of change management, particularly related to information governance improvement initiatives
- Understands current NHS policy and related regulation, and its implications for the delivery of healthcare services and information governance compliance
- Committed to improving the information governance of healthcare services
- Highly developed verbal and written communication skills
- Self-motivated, works well either independently or as part of a team
- Well-developed presentation skills
- Committed to continuing professional development

Desirable

- Experience of working in a fast-paced environment
- Experience of working within a Specialist Service e.g. (Children Services, Sexual Health, Dermatology, Prisons or MSK)
- Evidence of successfully handling sensitive situations effectively and confidentially
- Experience of working effectively in collaboration with other agencies
- Management of the Data Security & Protection Toolkit

- Experience of using OneTrust or other privacy management system

Employee signature

Manager signature