

Job Title:	Information Governance Compliance Lead
Reports to (job title):	Head of Information Governance
Line Manager to:	Senior DSAR Officer and team

Job purpose

This role supports the standard for information governance across the business and supporting teams to continuously improve information governance and data security across the organisation in our central function, business units and for our service users. The Information Governance (IG) Compliance Lead is responsible for managing a range of assurance activities in relation to UK Data Protection Laws, The Data Security & Protection Toolkit (DSPT) and the ICO Accountability Framework. This role will also provide support for the completion and submission of the DSPT toolkits and ensure the IG Risk Log is regularly reviewed and KPIs monitored and maintained.

Key responsibilities

The Information Governance (IG) Compliance Officer is responsible for managing a range of assurance activities in relation to data protection and information governance compliance such as The Data Security and Protection Toolkit (DSPT), the ICO Accountability Framework (AF) and other areas within the information governance framework.

This role will promote and lead the highest standards of information governance and data security, and continuous improvement through:

1. Working with the Head of Information Governance and Information Security Lead to:
 - a. Continue the development of the audit and assurance programme linked to the DSPT and Accountability Framework
 - b. Develop a compliance programme using Microsoft 365 data governance and compliance capabilities using Microsoft Compliance Manager and ServiceNow
 - c. Support further improvements through the introduction or alignment to information standards such as ISO27001 Information Security Standard and BS10012 – Personal Information Management System
 - d. Conduct audits and reviews in line with the audit and assurance programme
 - e. Produce risk based reports for stakeholders within the organisation and externally

where required. This includes the IG Committee and Records Group and overseeing the IG Advisors and IG Lead with their quarterly reports to ensure consistency in messaging and actions.

2. Carrying out monthly and reporting on incident monitoring meetings and trend analysis to enable actions to be developed to ensure incident reduction such as retraining, updates to policies and procedures and escalation or risk to the IG Committee.

3. Developing training and awareness programmes and communication to ensure best practice and learning is shared from incidents

4. Working with the IG Lead to jointly lead:

a. the programme of annual Records of Processing Activity Reviews ensuring OneTrust is maintained with accurate, up to date and risk assessed data flows and retention periods

b. The maintenance and preparation of draft Privacy Notices for DPO review prior to publishing ensuring children's services and prison healthcare are clear and meet the needs of the service users

5. Responsibility for DSPT submissions including:

a. Supporting the Primary Care Teams with the completion & submission of their toolkits, ensuring that dip sample reviews are conducted to provide assurance.

b. Working with the Head of IG and Security Lead and other stakeholders to gather and maintain robust evidence for the annual audit and submission to NHSX.

c. Assisting with the annual external audit(s)

6. Supporting the Head of Information Governance & DPO in developing the strategy and plans and processes to centralise access to records requests by:

a. Conducting a cradle to grave review of OneTrust prior to the Health Check process

b. Considering other options for managing requests and redacting safely

c. Carrying out a gap analysis on existing processes

d. Providing compliance reports where required

7. Providing day to line management the SAR Team Leader, proactively participating in management supervision, objective setting and appraisal process.

8. Assisting the Head of IG with all training requirements for the IG Advisors and their IG Data protection Apprentices

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.

Care

- Inspire
- Understand
- Communicate

Think

- Challenge
- Improve
- Learn

Do

- Accountability
- Involve
- 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 business

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.

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.

Personal Specification

Essential

A certified data protection or information governance qualification

- A minimum of 1 year's experience in working in a compliance role
- Comprehensive understanding of regulatory compliance and risk
- Experience of a lead change management role, 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
- The ability to act as a trusted advisor to the Head of Information Governance, providing confidence to the Caldicott Guardian and SIRO on all matters of information governance, risk, regulatory compliance and improvement using a highly supportive leadership approach
- Committed to continuing professional development

Desirable

- Experience of developing and delivery training and awareness programmes
- Well-developed presentation and media skills
- MS365 including SharePoint experience
- Experience in working in a management position in a health and care setting

Employee signature

Manager signature
