Title:	Data Protection Officer - DPO	Department:	Quality and Governance	Budget:	xx
Direct Reports:	None	Reports To:	Head of Regulatory and Compliance	Version:	V2

Role Purpose:	Key Accountabilities
To ensure LLOYDS CLINICAL fully discharges its duties in relation to compliance with data protection laws and the safeguarding of patients' personal data as defined by the General Data Protection Regulation (GDPR), the Data Protection Act 2018 and the Caldicott Principles (working in collaboration with the Caldicott Guardian).	1. Creating, owning and delivering an Information Governance (IG) framework for handling information in a secure and confidential manner allowing LLOYDS CLINICAL and its workers to manage patient, employee, personal and sensitive information legally, securely, efficiently and effectively 2. Creating, owning and delivering a set of policies and procedures that comply with the GDPR, the Data Protection Act 2018, and the Caldicott Principles ensuring all LLOYDS CLINICAL sites conduct their activities in accordance with the relevant legal requirements 3. Managing and conducting audits and assessments across all LLOYDS CLINICAL sites ensuring colleagues are continually improving in their overall IG compliance 4. Creating, owning and delivering a training and development framework that educates, develops and assesses all aspects of IG across all colleagues (and contractors) across all LLOYDS CLINICAL sites 5. Working collaboratively and proactively with internal and external stakeholders to maximise compliance and minimise risk

Key Accountabilities:	Key Measures of Success:
1. Creating, owning and delivering an Information Governance (IG) framework for handling information in a secure and confidential manner allowing LLOYDS CLINICAL and its workers to manage patient, employee, personal and sensitive information legally, securely, efficiently and effectively – Ensure the IG framework allows LLOYDS CLINICAL to fully discharge its responsibilities to safeguard data and protect employee and patient information and confidentiality – Develop and maintain standards that must be applied when information is processed in relation to how it is obtained, recorded, held, used and shared – Ensure all information is held securely and confidentially; obtained fairly and effectively; recorded accurately and reliably; used effectively and ethically; and shared appropriately and lawfully – Bring together all of the legal requirements, standards and best practice (including policies and procedures, management and reporting arrangements, processes and controls, auditing and training) that apply to the handling of patient, employee, personal and sensitive information, including but not limited to: – Access to Health Records Act	– All IG business objectives are achieved – All business areas pass the internal IG Audit – Mandatory training for IG is 100% up to date – IG breaches are contained and on a downward trajectory – IG risks to the business are comprehensively mitigated – Stakeholders suggest ways to improve IG within their department

– Caldicott Principles – Confidentiality: NHS Code of Practice – Data Protection legislation - UK Data Protection Act 2018 and the UK General Data Protection Regulation 2016 (GDPR) – Data Security and Protection Toolkit (DSPT) – Freedom of Information Act 2000 – Information Security Management: NHS Code of Practice – Network and Information Systems (NIS) Regulations 2018 – Records Management Code of Practice 2021. – Work closely with the IT and cybersecurity teams to ensure appropriate technical and organisational measures are in place to protect data from breaches – Ensure the confidentiality, integrity, and availability of information through encryption, access controls, and cybersecurity practices – Ensure that the large amounts of personal confidential data that is used by many colleagues in the course of their work every day is protected and kept safe – Support the Caldicott Guardian in applying the Caldicott Principles to safeguard patient confidentiality and ensure only authorised individuals have access to patient information on a need-to-know basis and facilitate appropriate and secure sharing of patient information between healthcare providers and organisations involved in the patient's care, while respecting patient consent and confidentiality – Ensure patients' rights regarding consent, access to their records, and requests for correction or erasure are respected and properly managed – Be the Information Governance representative at the Quality, Patient Safety and Risk Management Forum (QPSRM) – Review and provide feedback on data sharing agreements, contracts and other similar documentation and support tenders and bids – Advise SLT of any requests to transfer data outside of the UK Personally stay up-to-date with changes in the regulatory environment and provide guidance on compliance requirements which may involve working closely with legal and compliance teams to ensure adherence to applicable regulation	– IG KPI's are on the correct trajectory Positive feedback from SLT regarding IG risks on Corporate Risk Register
2. Creating, owning and delivering a set of policies and procedures that comply with the GDPR, the Data Protection Act 2018, and the Caldicott Principles ensuring all LLOYDS CLINICAL sites conduct their activities in accordance with the relevant legal requirements – Establish Information Governance policies and procedures for the creation, storage, retention, transfer and disposal of patient records in compliance with legal and regulatory requirements. This includes ensuring proper documentation, accurate record-keeping, and adherence to retention schedules. – Develop, implement, and maintain LLOYDS CLINICAL's data protection policies and procedures ensuring they are aligned with legal requirements and industry standards – Define policies for managing the lifecycle of records, including creation, retention, storage, and disposal – Implement a classification system to ensure data is categorised based on sensitivity, ensuring secure handling of confidential and sensitive information – Regularly review and update the data protection policies to address any regulatory changes, business developments, or emerging risks	– All data protection business objectives are achieved – All business areas pass the internal data protection audit/assessment – Mandatory training for data protection is 100% up to date – Data Protection breaches are contained and on a downward trajectory – Data Protection risks to the business are comprehensively mitigated

– Ensure compliance with the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and Caldicott Principles (working with the Caldicott Guardian) to protect patient and employee data and ensure it is processed lawfully and securely – Report on the management and compliance of IG to the SLT – Provide advice and guidance to the SLT, colleagues, and other relevant parties on matters related to data protection – Main point of contact for data subjects and providing information and assistance regarding data protection rights and obligations – Action subject access requests and other data subjects' rights and respond to Freedom of Information Requests that may arise from time to time – Develop clear protocols for sharing data with third parties, both inside and outside the UK, in compliance with data protection laws – Ensure that data sharing agreements are in place with third parties and that adequate security controls are enforced during data exchanges – Oversee compliance with regulatory frameworks, including Good Clinical Practice (GCP), Good Manufacturing Practice (GMP), and UK Medicines and Healthcare products Regulatory Agency (MHRA) regulations Regularly review LLOYDS CLINICAL's data security practices, particularly concerning sensitive health data, patient and employee records	– Stakeholders suggest ways to improve data protection within their department – Data protection KPI's are on the correct trajectory Positive feedback from SLT regarding data protection risks on Corporate Risk Register
3. Managing and conducting audits and assessments across all LLOYDS CLINICAL sites ensuring colleagues are continually improving in their overall IG compliance – Create a timetable of announced and unannounced audits across all LLOYDS CLINICAL sites ensuring the monitoring of compliance with Information Governance policies and to identify areas for improvement. This includes monitoring data access logs, conducting risk assessments, and responding to and reporting data breaches as required. – Conduct regular information risk assessments to identify, assess, and mitigate potential risks related to information handling and security – Implement Data Protection Impact Assessments (DPIAs) for high-risk data processing activities, ensuring that data protection risks are identified and minimised – Implement risk assessments, especially for sensitive or critical information assets, and establish incident management processes to handle data breaches – Implement procedures for detecting, reporting, and responding to data breaches or other information governance incidents – Conduct local data privacy impact assessments, legitimate interest assessments (where applicable), reviewing data protection practices, and ensuring that appropriate safeguards are in place. Support the maintenance, accuracy and accessibility of patient facing materials such as the LLOYDS CLINICAL Privacy Statement. – Ensure compliance with mandatory reporting requirements, such as notifying the Information Commissioner's Office (ICO) within 72 hours of a data breach where applicable – Conduct root cause analysis, implement CAPA's and post-incident reviews to prevent reoccurrence – Identify and manage risks associated with the collection, storage, and processing of patient information, including potential breaches, data loss, and system vulnerabilities – Ensure compliance with data retention schedules based on regulatory and business requirements, while ensuring secure destruction when data is no longer needed – Monitor for data breaches and ensure that procedures are in place to detect, investigate, and respond to data security incidents	– All risk management business objectives are achieved – All business areas pass the internal risk management audit/assessment – Mandatory training for risk management is 100% up to date – Risks are contained and on a downward trajectory – Stakeholders suggest ways to reduce risks within their department – Risk management KPI's are on the correct trajectory Positive feedback from SLT regarding how risks are managed and contained on Corporate Risk Register

– Main point of contact for the supervisory authority (Information Commissioner's Office) and must co-operate with the authority, respond to inquiries, and assist in any investigations or audits related to data protection. Ensure LLOYDS CLINICAL's entry on the ICO register is maintained – Manage the process for notifying the Information Commissioner's Office (ICO) and affected individuals in the event of a data breach within the required 72-hour time frame Establish and maintain procedures for detecting, reporting, and investigating breaches. In case of a data breach (or near miss), assess the risks, notify the supervisory authority (Information Commissioner's Office), and communicate with affected individuals when necessary	
4. Creating, owning and delivering a training and development framework that educates, develops and assesses all aspects of IG across all colleagues (and contractors) across all LLOYDS CLINICAL sites – In collaboration with Learning and Development create, deliver and facilitate workshops or/and training/on-line sessions to enhance Information Governance and Data Protection capabilities ensuring compliance and minimising the risk of data breaches across all LLOYDS CLINICAL sites – Provide regular training, utilising NHS toolkit, to colleagues (and contractors) on the Information Governance Principles, Data Protection obligations, Caldicott Principles and security best practices – Ensure all colleagues (and contractors) understand their responsibilities in protecting data and complying with relevant regulations – Maintain a strong culture of Information Governance, including Caldicott Principles, Data Protection and GDPR compliance across all LLOYDS CLINICAL sites in order to deliver service excellence – Ensure all colleagues understand their Information Governance responsibilities and follow best practices whilst handling personal data – Raise the general awareness of IG across all LLOYDS CLINICAL sites and whilst promoting a risk-aware culture Ensure all mandatory training relating to IG is completed across all LLOYDS CLINICAL sites	– All colleagues are aware of the high level IG, data protection and risk management business objectives – Mandatory training for IG is 100% up to date – Stakeholders suggest ways to reduce risks and improve compliance with IG and data protection within their department
5. Working collaboratively and proactively with internal and external stakeholders to maximise compliance and minimise risk – Build strong and collaborative relationships with key colleagues including, but not limited to: – Information Services – Patient Services – The Caldicott Guardian – Nursing and Safeguarding – Quality and Governance team – Collaborate with internal and external stakeholders to gather information, assess risks, and implement risk mitigation measures and liaise with departments, business units, and external partners to ensure a comprehensive and co-ordinated approach to risk management. – Work in collaboration with other departments to manage cybersecurity, financial risk, and operational risk, based on LLOYDS CLINICAL's needs. – Promote a privacy-by-design approach across all LLOYDS CLINICAL sites, being involved in assessing the impact of new projects or initiatives on data protection, conducting DPIAs, and recommending measures to mitigate risks.	– Positive feedback from stakeholders IG, data protection and risk management business decisions are made based on an inclusive basis

– Participate in business continuity planning and help develop strategies to ensure LLOYDS CLINICAL's resilience in the face of potential risks and disruptions which includes developing business continuity plans, crisis management protocols, and recovery strategies – Implement appropriate technical and organisational measures to protect patient data from unauthorised access, disclosure, alteration, or destruction. This includes ensuring the use of secure IT systems, encryption, access controls, and colleague training on security practices. – Carry out other duties that may be required from time to time.	

Enablers to the Role (Skills, Knowledge, Experience)

Skills

- Ability to perform duties independently and should not receive any instructions regarding the execution of tasks
- Ability to monitor the organisation's compliance with data protection laws, regulations, and internal policies related to data protection
- Strong communication skills to effectively interact with colleagues, management, and data protection authorities and making recommendations
- Strong analytical skills are crucial
- Adept at identifying potential issues and developing strategies to mitigate them
- Proficiency with relevant software tools, data analysis, and risk assessment tools can be beneficial
- Ability to adapt to changing circumstances and emerging risks is important
- Ability to work within teams and collaborate with different departments to ensure a comprehensive approach to managing data is achieved

Knowledge & Qualifications

- Certification in the field of Data Protection
- Strong understanding of the Data Protection Act 2018 and GDPR and other relevant data protection regulations
- Knowledgeable about conducting Data Protection Impact Assessments (DPIAs) and should be able to assist the organisation in assessing the impact of data processing activities on individual privacy
- Good understanding of the organisation's structure, activities, and data processing operations

Experience

- Professional experience in data protection and privacy matters
- Experience in Data Protection Law and Practices
- Experience of auditing businesses and providing reports with recommendations for improvement
- Experience of creating and delivering training courses
- Experience of creating and presenting reports for SLT

Some experience of working with a Caldicott Guardian is preferred