Deer Park Family Medical Practice

Roles and Responsibilities for Information Governance

Named Individuals

The Practice Information Governance Lead is Casey Bond
The Practice Caldicott Guardian is Dr William Tao
The Practice Digital Safety Officer is Dr William Tao
The Practice Data Protection Officer is Paul Couldrey of PCIG Consulting Limited.

Their Roles and responsibilities are listed below

Information Governance Lead

The IG Lead is the overall Information Governance Lead for the Practice and will lead on Caldicott, Data Protection and Freedom of Information issues.

As Information Governance Lead, their main responsibilities for Information Governance will be:

1. ensure there is an up-to-date IG policy in place;
2. ensure that the organisation's approach to information handling is communicated to all staff and made available to the public.
3. coordinate the activities of staff given data protection, confidentiality and Freedom of Information Act responsibilities;
4. monitor the organisation's information handling activities to ensure compliance with law and guidance;
5. ensure staff are sufficiently trained to support their role;
6. ensure that the organisation submits their annual DS&P Toolkit assessment;
7. support monitoring visits from the commissioning organisation (where appropriate).
8. Ensure that IG is regularly discussed in Practice meetings.

The IG Lead will also lead on: -

- Maintaining an IG action plan for the practice and ensure an improvement plan is followed
- Assist with investigations into complaints about breaches of confidentiality, the Data Protection Act 2018/ UKGDPR 2016 or Freedom of Information Act 2000 and undertake reporting/remedial action as required. Maintain a log of any incidents and remedial recommendations and actions.
- Provide advice to the Practice on Information Governance issues

Caldicott Guardian

A Caldicott Guardian is a senior person within a health or social care organisation who is responsible for ensuring that confidential patient and service user information is used ethically, legally, and appropriately. They act as the organisation's "conscience" for data sharing, advising on ethical and legal considerations to uphold patient confidentiality while also enabling the responsible use of data to improve care and services.

Key Responsibilities:

- **Advising on ethical and legal matters:**

  Providing leadership and guidance on complex cases involving confidential information, especially when the correct course of action isn't immediately clear.

- **Upholding Caldicott Principles:**

  Ensuring the organisation follows the eight principles established for the ethical and legal use of patient-identifiable information.

- **Ensuring appropriate information sharing:**

  Working to enable the lawful and ethical sharing of information when it's necessary to improve patient care, as well as protecting confidentiality.

- **Promoting high standards of data handling:**
  Ensuring the organisation's policies and practices for handling personal information meet high standards for confidentiality.

Who they are:

- **Senior individuals:**

  They are senior figures, such as a medical director in some cases, to provide the necessary authority and insight.

- **Mandatory in certain organisations:**

  Since 2002, all NHS organisations and local authorities providing social services have been required to have a Caldicott Guardian.

- **Supported by a council:**
  The Caldicott Guardian role is supported by the UK Caldicott Guardian Council, providing guidance and standards for their work.

The Caldicott Guardian will:

- Act as the ‘conscience’ of the Practice by actively supporting work to facilitate and enable information sharing whilst advising on options for lawful and ethical processing of information as required

- Champion Information Governance Requirements at Practice level

- Ensure that confidentiality issues are appropriately reflected in organisational policies and working procedures for staff

- Oversee all arrangements, protocols and procedures where confidential patient information may be shared with bodies both within and outside the NHS.

- Be consulted where necessary on information requests, typical examples being:

    - a request from the police for access to patient information
    - requests from patients to delete information from their records
    - an actual or alleged breach of confidentiality

Digital Safety Officer

An NHS Digital Safety Officer (DCSO) is a senior clinical professional responsible for ensuring digital health systems and applications are safe for patient care. Key requirements include clinical registration with a professional body like the GMC or NMC, and expertise in clinical safety and risk management. The role involves managing clinical risks associated with digital systems throughout their lifecycle, promoting safe digital adoption, overseeing safety assurance processes, and providing training to foster a strong safety culture.
Role and Responsibilities

- **Clinical Safety Oversight:**

  Ensure digital clinical safety is a central priority in all digital transformation and change management projects.

- **Risk Management:**

  Develop, maintain, and refine processes for identifying and addressing clinical safety risks in digital health applications and IT systems.

- **System Assurance:**

  Manage and oversee the safety assurance of health IT software, ensuring manufacturers and other organizations meet required safety standards.

- **Training and Culture:**

  Provide clinical risk management training to manufacturers and care organizations to promote a positive organizational safety culture.

- **Lifecycle Management:**

  Establish and maintain business processes for managing clinical safety risks for digital systems from procurement to decommissioning.

- **Collaboration:**
  Work with project managers, clinicians, and other stakeholders to ensure digital systems are safe and enhance patient outcomes.

Requirements and Qualifications

- **Clinical Registration:** Must be a senior clinician with current registration with a professional body, such as the General Medical Council (GMC) or the Nursing and Midwifery Council (NMC).
- **Clinical Safety Expertise:** Possess significant training and experience in clinical safety and clinical risk management.
- **Leadership and Management:** Experience in leadership and management is often a requirement.
- **Education:** A postgraduate qualification, such as a Masters or diploma in a relevant subject like Occupational Safety and Health, or equivalent knowledge and skills gained through experience, may be required.
- **Training:** Completion of specific training, such as the Digital Clinical Safety Intermediate e-learning and the Practitioner course, is necessary.
- **Professional Development:** A record of continuous professional development is essential.

Data Protection Officer

A Data Protection Officer (DPO) is an expert within an organisation responsible for ensuring compliance with data protection laws, such as the UK GDPR. Their tasks include informing and advising the organisation on data protection obligations, monitoring compliance with regulations, providing advice on Data Protection Impact Assessments (DPIAs), and acting as a point of contact for data subjects and the relevant supervisory authority, like the Information Commissioner's Office (ICO).DPOs must be independent, adequately resourced, and report to the highest management level.
Key Responsibilities

- **Inform and Advise:**

  They provide guidance and information to the organisation and its employees about their data protection obligations and how to comply with relevant laws.

- **Monitor Compliance:**

  The DPO monitors the organisation's internal adherence to data protection policies and regulations.

- **Advise on DPIAs:**

  They offer advice on Data Protection Impact Assessments (DPIAs), a crucial tool for assessing and mitigating data privacy risks.

- **Serve as a Contact Point:**

  DPOs act as a primary contact for individuals whose data is being processed (data subjects) and for the official supervisory authority, such as the ICO in the UK.

- **Ensure Independence:**
  DPOs must operate independently, without fear of penalty or dismissal for performing their duties.

The Practice DPO will also:

- Educate the company and employees on important compliance requirements
- Training staff involved in data processing
- Conducting audits to ensure compliance and address potential issues proactively
- Serving as the point of contact between the company and UK GDPR Supervisory Authorities
- Produce and manage assurance for all practices required Governance policies, Processes, procedures, and patient information to comply with UK GDPR, DPA2018 and the DS&P Toolkit requirements
- Provide Document templates for practices DS&P Toolkit submission
- Provide a Dedicated helpdesk call facility.
- Provide Practice updates
- Provide the Management and Reporting of all IG SIRI's and ICO communication

Name	Role	Signature

Date: 26/09/2025
Review Date: September 2028