Roles and Responsibilities for Information Governance/ Data Security and Protections Requirements – Practice Statement

PM is the overall Information Governance Lead for the Practice and will lead on Data Protection, data security and Freedom of Information issues.

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

- ensure there is an up to date data security and protections policy and associated policies in place, and available to staff;
- ensure that the organisation's approach to information handling is communicated to all staff and made available to the public;
- ensure that all personal confidential data is handled, stored and transmitted securely. Personal confidential data is only shared for lawful and appropriate purposes.
- Ensure all staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their personal accountability for deliberate or avoidable breaches.
- Ensure All staff complete appropriate annual data security training and pass a mandatory test.
- Ensure and monitor that Personal confidential data is only accessible to staff who need it for their current role. All access to personal confidential data on IT systems can be attributed to individuals.
- Ensure all data processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses.
- Ensure Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss.
- Ensure a continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum.
- Ensure No unsupported operating systems, software or internet browsers are used within the IT estate.
- Ensure that a strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

- Coordinate the activities of staff given data protection, confidentiality and Freedom of Information Act responsibilities;
- monitor the organisation's information handling activities to ensure compliance with law and guidance;
- ensure staff are sufficiently trained to support their role;
- ensure that the organisation submits their annual DS&P Toolkit assessment;
- support monitoring visits from the commissioning organisation (where appropriate).
- Ensure that IG is regularly discussed in Practice meetings

The Caldicott Guardian for the Practice is Dr Kendall as the practice 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 Caldicott 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

- Ensure that the Caldicott Principles within the Practice activities are complied with as below: -

    Principle 1 - Justify the purpose(s) for using confidential information

    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

The Appointed Data Protection Officer (DPO) defined in the General Data Protection Regulations 2016 (*Regulation (EU) 2016/679 On the protection of natural persons with regard to the processing of personal data and on the movement of such data*), Article 37 for the practice is Paul Couldrey, DPO, PCIG consulting Ltd. As the DPO Paul will:

- inform and advise the practice and the employees undertaking processing of their obligations pursuant to GDPR and to other data protection provisions ('other DP provisions')

- monitor compliance with GDPR and other DP provisions and with practice policies in relation to protection of Personal Data, including assignment of responsibilities, awareness-raising and training of staff and related audits.

- provide advice where requested about Data Protection Impact Assessments (DPIA) and monitor performance pursuant to Art 35 of the GDPR

- cooperate with the Office of the Information Commissioner Office (GDPR supervisory authority) and act as the point of contact with the ICO.

- act as contact point for ICO on issues relating to processing, including the prior consultation referred to in Art 36 and to consult, where appropriate, on any other matters

- Manage the reporting of any Data Protection Breaches to the ICO within 72 Hours of having become aware of it in accordance with Art 33

- Provide Breach reporting, investigation and lesson learnt reporting back to the practice in accordance with NHS standards.

- Ensure that the practice complies with the GDPR and Data Protection Act 2018.

The Senior Information Risk Officer (SIRO) for the Practice is [Name of SIRO] as the practice SIRO, [Name of SIRO] will:

- ensures the Organisation has a plan to achieve and monitor the right IG culture, across the Organisation and with its business partners;
- takes visible steps to support and participate in that plan (including completing own training);
- ensures the Organisation has appointed Information Asset Owners (IAOs) who are skilled, focussed on the issues, and supported, plus the information risk management specialists that it needs
- ensures that the organisation information risk policy is complete – covering how the organisation implements Information Governance risk management in its own services and activities and those of its delivery partners, and how compliance will be monitored
- ensures that information asset risk reviews are completed each quarter taking account of extant Information Governance guidance (available from DHSSPS)
- based on the information risk assessment, understands what information risks there are to the organisation and its business partners through its delivery chain, and ensures that they are addressed, and that they inform investment decisions including the risk considerations of outsourcing

- ensures that information risk assessment and mitigating actions taken benefit from an adequate level of independent scrutiny
- receives annual assessment of performance, including material from the IAOs and specialists, covering Information Governance reporting requirements as well as local actions planned for the organisation's own circumstances;
- provide advice to the Partners on the information risk parts of their Statement of Internal Control;