Data Protection Officer (DPO) – assignment of responsibilities between NHS Kernow and Cornwall and Isles of Scilly GP Practices

The Purpose of the Data Protection Officer (DPO) is to provide each organisation with independent risk-based advice to support its decision-making in the appropriateness of processing personal and special categories of data within the principles and data subject rights laid down in the General Data Protection Regulation (GDPR) and data protection (DP) legislation.

Responsibilities assigned to for the NHS Kernow CCG DPO role
• To provide a named DPO and champion/point of contact for GP practices in Cornwall and the Isles of Scilly • To maintain a comprehensive knowledge of GDPR and DP requirements • To inform and advise practices about the obligations to comply with GDPR and other data protection laws • To be responsive and provide timely advice on complex data protection issues, such as subject access requests, procurement decisions, information sharing and seek support from CITS for information/cyber security related issues • To promote a data protection culture actively raising awareness and alerting practices to new developments, known issues, best practice • To provide risk-based advice to practices • To advise on data protection policies and data protection impact assessments, when needed • To provide collective training sessions, practical advice and ongoing support to GP practices in response to new DP/GDPR requirements • Annual workshop to identify and improve processes including areas which have caused breaches or near misses or which force practice staff to use workarounds which compromise data security • Advice to support practices develop and maintain best practice processes that comply with national guidance on citizen identity verification • Advice to support practices achieve mandatory compliance with the National Data Opt-Out policy by March 2020 • To develop and manage a governance structure to record data protection advice and resulting decisions offered by the CCG
Responsibilities for individual GP practices
• To monitor compliance with the GDPR and other DP laws, manage internal data protection activities, raise awareness of data protection issues and conduct appropriate internal audits • Promote an appropriate data protection culture within the practice • To provide general DP training to staff to ensure the Data Security and Protection (DSP)Toolkit essential requirements are met, maintaining and co-ordinating a training matrix • To implement and monitor data protection impact assessments • Be the first point of contact for the Information Commissioners Officer (ICO) • Sign-off their own regulatory requirements, e.g. DSP Toolkit submissions • Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.) • Maintain a log of advice requested from DPO and actions taken • Have sufficient staff and resources to discharge their responsibilities under GDPR and data protection laws
Joint responsibilities
• Agree organisational trigger-points for mandatory input from the DPO