

Does the PCT have a confidentiality code of conduct that provides staff with clear guidance on the disclosure of patient personal information?

Requirement Attainment Levels
Attainment Level 0 The PCT does not have a confidentiality code of conduct for staff.
Attainment Level 1 The PCT has a confidentiality code of conduct for staff that provides clear guidance on the disclosure of patient personal information and has been approved by the Board, or delegated sub-group.
Attainment Level 2 The PCT has a confidentiality code of conduct for staff that provides clear guidance on the disclosure of patient personal information and has been approved by the Board, or delegated sub-group. The code has been made available across the PCT and all staff have been effectively informed about the guidelines and the need to comply with them.
Attainment Level 3 The PCT's approved confidentiality code of conduct has been made available across the PCT, all staff have been effectively informed about the guidelines and compliance with the code is monitored. The code incorporates sections tailored to specific staff groups or work locations where appropriate.

Has the PCT ensured that all person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines?

Requirement Attainment Levels
Attainment Level 0 The PCT does not know whether or not personal data about patients or staff is transferred from the PCT to countries outside of the UK.
Attainment Level 1

The PCT has carried out an assessment to determine whether it transfers personal data about patients or staff to countries outside the UK and whether any such transfer complies with the Data Protection Act 1998 and Department of Health guidelines.

Attainment Level 2

The PCT has assessed all transfers of personal data from the PCT to contractors in countries outside of the UK and ensures that the Data Protection Act 1998 and DH guidelines are fully complied with.

Attainment Level 3

The PCT regularly reviews its transfers of personal data about patients or staff to non-UK countries and ensures continuing compliance with the Data Protection Act 1998 and DH guidelines.

Does the PCT ensure that all new processes, software and hardware, comply with confidentiality and data protection requirements?

Requirement Attainment Levels

Attainment Level 0

The PCT has not established and/or documented a mechanism for ensuring that all new processes comply with confidentiality and data protection requirements.

Attainment Level 1

The PCT has established an appropriate documented mechanism for considering the compliance of new processes with confidentiality and data protection requirements.

Attainment Level 2

The PCT has established an appropriate documented mechanism for considering the compliance of new processes with confidentiality and data protection requirements and all staff who may introduce these are aware of the approval process.

Attainment Level 3

The PCT identifies and reviews all new processes to ensure that they comply with confidentiality and data protection requirements. All staff who may introduce these comply with the approval process.

Does the PCT ensure that operating and application information systems under its control support appropriate access control functionality?

Requirement Attainment Levels
<p>Attainment Level 0 The PCT does not ensure that operating and application information systems under its control support appropriate access control functionality.</p>
<p>Attainment Level 1 The Information Asset Owners responsible for each asset have documented action plans that define and document requirements for access controls affecting their information assets.</p>
<p>Attainment Level 2 The PCT Information Asset owners have implemented their action plans to apply appropriate access control functionality for assets under their control in line with the PCT Information Risk Policy. IAOs ensure that access is only granted to individuals who have been duly authorised and ensure appropriate technical functionality and management controls exist to support and maintain this.</p>
<p>Attainment Level 3 The PCT IAOs ensure appropriate access control functionality is implemented for all information assets under their control and that regular reviews are made of the effectiveness of these controls. Additionally, there is a PCT-wide programme in place to audit and assure the access control and management processes (e.g. reviewing password configuration settings, password cracking, penetration testing etc) and to undertake any remedial/improvement activities that may be necessary. Regular reports are provided to the PCT SIRO.</p>

Does the PCT have appropriate procedures in place to ensure that communication networks under the PCT's control operate in a secure manner?

Requirement Attainment Levels

Attainment Level 0

The PCT has yet to define the controls required to manage its network and put in place action plans to implement these controls.

Attainment Level 1

The PCT has documented the controls required to manage its network(s), through its information security policy, supporting procedures and its risk management plan etc. It has put in place action plans to implement these controls.

Attainment Level 2

The PCT has implemented the required controls as documented in its network security policy, supporting procedures and risk management plan etc.

Attainment Level 3

The PCT regularly monitors compliance with its information security policy, commissions operational and technical audits (e.g. from internal audit) of the network, including penetration tests and in all instances acts upon findings to take remedial or improvement action.

Does the PCT have in place appropriate procedures for ensuring that the development and introduction of any new Information Systems, or other relevant Information Assets of the PCT are conducted in a secure and structured manner? This requirement includes the development and maintenance of appropriate IG accreditation documentation.

Requirement Attainment Levels

Attainment Level 0

The PCT does not have a documented approach to the management of projects, which requires the definition of security requirements and ensures robust changes control processes.

Attainment Level 1

The PCT has a documented and approved approach to the management of its local IT projects which requires the definition of information security requirements at an early stage of the project cycle and ensures robust change control processes.

Attainment Level 2

The PCT ensures that all systems implementations follow the documented project management process with security requirements having been defined and selected, and security related risks and issues having been identified and addressed as part of the lifecycle process. Robust change control processes have been applied.

Attainment Level 3

The PCT ensures that project assurance processes are in place and the results are fed through project boards or similar groups. Remedial or improvement action is documented and taken where appropriate.

Does the PCT have appropriate procedures for ensuring that mobile computing and teleworking are conducted in a secure manner?

Requirement Attainment Levels**Attainment Level 0**

The PCT does not have an authorisation procedure for mobile/teleworking, has not introduced appropriate authentication procedures, nor guidelines for staff on expected NHS IG information security and confidentiality practice.

Attainment Level 1

The PCT has documented an authorisation procedure for mobile or teleworking, has implemented appropriate approvals and authentication procedures, and has guidelines for staff on expected NHS IG information security and confidentiality practice.

Attainment Level 2

The PCT ensures that all mobile or teleworkers are appropriately approved, authorised and records maintained of all authorisations. Robust remote access solutions and information security for mobile devices and removable media have been provided and users have been effectively instructed in their use.

Attainment Level 3

The PCT undertakes regular audits of remote and/or teleworking arrangements ensuring that all users are approved, that assets can be accounted for, that secure remote access is used, and that any sensitive or confidential information is securely transported or stored in the remote location. Appropriate remedial or improvement action is documented and taken where appropriate.

Does the PCT ensure that Registration Authority equipment (hardware and software) and consumables meet current specifications, is adequately maintained and securely stored?

Requirement Attainment Levels

Attainment Level 0

The PCT has not yet assessed its equipment requirements for RA or developed a policy for maintaining and securing RA equipment and consumables.

Attainment Level 1

The PCT has assessed its RA equipment needs and has identified any shortfalls in existing equipment or specification and the measures to be taken to address these shortfalls. A policy for maintaining and securing RA equipment has been drafted.

Attainment Level 2

The PCT has implemented its RA equipment policy and has the necessary equipment in place to fulfil its role as a Registration Authority. Procedures for the ongoing use and maintenance of the equipment and for the control of documentation, smartcards etc. have been established.

Attainment Level 3

The PCT has implemented its RA equipment policy and has the necessary equipment in place to fulfil its role as a Registration Authority. Procedures for auditing equipment hardware and software, including controls over RA forms and smart cards have been established and regular audits effected.

Does the PCT have robust procedures and processes for monitoring all data collection activities across the PCT?

Requirement Attainment Levels

Attainment Level 0

The PCT has no procedures and processes for monitoring data collection activities.

Attainment Level 1

The PCT has documented and approved procedures and processes for monitoring data collection activities.

Attainment Level 2

The PCT has implemented the documented procedures and processes for monitoring data collection activities across the organisation and ensures that queries about data identified by

validation and/or from internal recipients are logged and responded to within locally agreed timescales.

Attainment Level 3

The PCT has documented and implemented procedures for monitoring all data collection activities across the organisation and ensures that timescales for the correction of errors are consistently met and that synchronicity between separate databases is maintained. The effectiveness of the procedures and processes is monitored through regular sample checks.

Does the PCT have procedures in place to ensure that when new services are provided, or where changes within the system are made, that these do not adversely impact on information quality?

Requirement Attainment Levels

Attainment Level 0

The PCT has no procedures in place to ensure that adverse impact on information quality is prevented when new services are provided, or where changes within the system are made.

Attainment Level 1

The PCT has documented and approved procedures that aim to ensure that there is no adverse impact on information quality when new services are provided, or where changes within the system are made.

Attainment Level 2

The PCT has implemented the approved procedures to reduce any risk of an adverse impact on information quality when new services are provided, or where changes within the system are made. The procedures are available in every area where new services or changes in the system may be developed and relevant staff have been effectively informed of the need to comply with them.

Attainment Level 3

The PCT monitors and enforces compliance with the approved procedures to ensure that there is no adverse impact on information quality when new services are provided, or where changes within the system are made. Evidence of non-compliance is investigated and appropriate action taken.