

1.21.4 Control of Personal Confidential Information

Please advise how is access to person confidential data (PCD) held by your organisation will be controlled and managed in your proposed approach?

(Maximum Word Count 500 words plus relevant attachments)

Words used = 500

1.21.4.1-Key roles

All users are responsible for ensuring the security of PCD. The Data Protection Officer ensures compliance with the GDPR and internal data protection policies.

Vocare complies with all relevant IG requirements:

- GDPR
- DPA 2018
- ICO GDPR guidance
- IGA data-protection guidance
- ISO27001:13 accredited,
- Working towards NHSD DCB1596 Accreditation and Cyber Essentials

Accountable roles:

- | | |
|--|---------------------------------|
| • Senior Information Risk Owner [SIRO] | Managing Director |
| • Information Risk Owner [IRO] | Head of Corporate Assurance |
| • Data Protection Officer [DPO] | Director of Corporate Assurance |
| • Caldicott Guardian | Medical Director |

1.21.4.2-Policies, procedures and training

V-G 966 Data Protection Handbook, associated policies and procedures are designed to ensure organisational and personal compliance with GDPR regulations.

All policies are held centrally under version control with defined review/end dates, accessible to staff via the Vocare intranet. Incidents, complaints, claims, internal or external process or legislation changes will trigger earlier review.

The document controller circulates a weekly email summary of new or revised policies. Obsolete documents are archived as per our records retention policy.

Role specific requirements are defined in the organisations training needs analysis.

NHS Data-Security Awareness L1 course is mandated at induction and annually for all staff. Service Managers and the Executive complete DPO-delivered training covering their responsibilities. Fortnightly Executive-Team reviews track training completion.

1.21.4.3-Controlling access to PCD

- Patient records access - limited to staff providing patient care and/or management, controlled by individual login in accordance with our Access Control Policy. Adastra records full audit trail of individual user activity.
- Access to appropriate Adastra functionality – controlled by user roles, defined by skillset.
- Adastra delivered using Citrix - all data stored on secure data-centre servers.
- Locally held PCD - limited to clinical-governance information [audits, incidents, complaints] stored on secure servers.
- Centrally controlled IT policy - prevents the use of USB devices and home printers.
- Laptop and mobile phone – require signed user agreements. Leaver's checklist ensures equipment is returned prior to employees leaving the organisation.
- Physical building access - via key fob or secure code. Visitor Policy ensures control of assets and information held on site.
- PCD transmission - encrypted, or pseudo anonymised data, sent via NHS email or approved secure data transfer methods.
- Faxing - for recipients with safe-haven facilities where no other method available [pharmacies without EPS].
- Transportation of PCD documentation - using carrycases with inventoried contents [contingency only process]
- Managing access to PCD

a)-Audit

Scheduled audits assess compliance, action plans implemented to address any issues.

- Patient-data usage [monthly, internal]
- Data security toolkit submission [annually]
- BSI audit for ISO 27001 [annually]

b)-Breaches

IG-related incidents are logged and managed using Datix, escalating/reporting according to policy. Serious Case Incidents Finding (SCIF) meetings conducted for any red-flag incidents. Incidents are discussed at local daily risk / monthly governance meetings and reported on contract performance reports. Outcome reviews ensure continuous improvement. Where involved, ICO has never taken enforcement action.

c)-Subject Access Requests

Strict adherence to authorisation for governance processes ensures senior level oversight [SARs, legal correspondence, police/other third-party requests, safeguarding, complaints]. SARs are assessed by Head of Governance and reviewed by Head of Corporate Assurance.