

1.21.5 Transfer of Personal Confidential Information

Please advise how your organisation proposes to facilitate the transfer of person confidential data (PCD) into and out of your organisation?

(Maximum Word Count 500 plus relevant attachments)

Words used = 500

1.21.5.1-Key roles

All users are responsible for ensuring safe transfer of PCD. The Data Protection Officer ensures compliance with 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 officers

- | | |
|--|---------------------------------|
| • 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 |

1.21.5.2-Policies, procedures and training

Vocare have a set of policies and training supporting Transfer of Personal Confidential Data.

V-IG P1020 Secure Data Transfer Policy details the approved secure methods of data transfer, referencing relevant related policies and procedures.

All policies are accessible to staff via the Vocare intranet. They are held centrally under version control, with defined review/end dates. 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.

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

NHS Data-Security Awareness course is mandated at induction and annually for all staff, completed via the e-Learning for Health portal. Service Managers and the Executive complete DPO-delivered training covering their responsibilities.

Fortnightly Executive-Team reviews track training completion.

1.21.5.3-Data sharing

Vocare use **Data Sharing Agreements** (DSAs) to define what data is shared and how it will be used, any third-party contracts include additional clauses outlining requirements for securely handling PCD.

DSAs are in place to manage our existing Staffordshire contract.

A **Data Protection Impact Assessment** will be undertaken during mobilisation to identify any risks. We will sign new/revised agreements with organisation to meet the requirements of the new service.

1.21.5.4-Transfer of PCD into Vocare

PCD is transferred into Vocare for the following purposes:

- Patient referrals or booked appointments from NHS-111 and NHS111 Online
- Receipt of Health Professional Feedback Forms (HPFFs)
- Subject Access Requests (SARs)

Accepted PCD transfer methods are:

- NHS Interoperability Toolkit (ITK) secure message
- NHS email
- Interlinkage (Adastra to Adastra)

1.21.5.5-Transfer of PCD from Vocare

Vocare transfer PCD outside of the organisation for the following purposes:

- Patient referrals, appointment booking and prescription request
- Ambulance dispatch
- KPI reporting
- PEMS / discharge summaries to GP practices
- Complaint's handling
- Management of HPFFs
- SARs response
- Legal documentation such as claims, including to NHS Resolution
- Management of the contract
- Commissioner requests

All PCD is transmitted using encrypted, or pseudo anonymised data, sent via NHS approved secure data transfer methods:

- NHS Interoperability Toolkit (ITK) secure message
- NHS Electronic Prescription Service (EPS)
- DTS secure messaging / email
- Docman Connect

- NHS email

Faxing is used for recipients with safe-haven facilities where no other method is available [e.g. pharmacies without EPS].

Transportation of printed documents containing PCD by carrycase with inventoried contents is used for contingency, for example where a clinician could not access the system during a home visit and returns to base to update consultation notes on Adastra.

No PCD is transmitted outside of the EU.