

1.21.1 Implementation of Information Governance

Please provide details of the technical and physical measures in place to ensure the security of any person confidential data (PCD) held by your organisation (both physical and electronic information), including details which relate to staff accessing data from their residence (home working) where applicable.

(Maximum Word Count 500 plus relevant attachments)

Words used = 440

Vocare complies with all relevant IG requirements.

- GDPR
- DPA 2018
- ICO GDPR guidance
- IGA data-protection guidance

ISO27001:13 accredited and working towards NHSD DCB1596 Accreditation and Cyber Essentials

1.21.1.1-Key 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 |

1.21.1.2-Policies and procedures

V-IG 972 Information Security Employee Handbook summarises relevant policy requirements, referencing the full documents.

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 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.

1.21.1.3-Technical and physical measures to ensure PCD security

System-security features for Adastra, Datix, QUINCYX (rotas), SAGE (payroll) include:

- Securely hosted UK data warehouses.

- Encrypted data transmission
- HSCN/N3 network access
- Individual-user password protection for telephone and system access
- Encrypted secure NHS-email platform

a)-Telephone consultations

When calling patients Demographics are checked to confirm patients' identity. (auditable in the monthly call audit process). Voice message etiquette ensures confidentiality is maintained.

b)-Face-to-face consultations

All consultations, including video, are conducted in private rooms.

Reception and consultation room computer screens face away from the patients or use privacy screens where this is not possible. Screens are locked automatically after a period of inactivity or manually by the user when leaving the room unattended.

Virtual consultations via Q-Doctor, an NHS Digital approved secure video solution.

c)-Home visits

Consultations are conducted privately unless the patient requests a family member, friend, or carer present. Consultation notes are updated electronically on Adastra.

d)-Home working

Our home working policy requires line manager approval, subject to employee self-declaration confirming:

- Use of a private, enclosed, undisturbed room where they cannot be overheard
- Understanding of their personal liability under the Data Protection Act 2018
- Laptops will be locked when unattended

Vocare laptops are configured with 'always on' SSL VPN (encrypted Virtual Private Network) providing secure connection to Adastra. Secure logon is via Active Directory account and two-factor code generated via Google Authenticator. BitLocker encryption and PIN code entry at start-up prevent access to any locally stored data by another device.

1.21.1.4-Data protection track record

Our robust processes has ensured only two security incidents referred to ICO, with no further action needed.