

1.21.3 Remote Contacts

Describe how you ensure safe and secure practice when delivering remote and virtual patient contacts, including how clinical notes are recorded.

(Maximum Word Count 500 plus relevant attachments)

Words used = 499

1.21.3.1-Key roles

All staff are responsible for ensuring safe and secure practice during remote and virtual patient contacts.

Day-to-day services are overseen by the Area leadership team (Clinical, Operations and Medical Directors and Governance team) supported at regional level by the Regional Director and Head of Quality and Governance.

The National Clinical Assessment Service (NCAS), a specialist team of remote GPs and Advanced Practitioners, are managed by dedicated medical, clinical and operational leads.

Vocare complies with all relevant IG requirements and legislation:

- 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 |

1.21.3.2-Policies, procedures and training

All policies are accessible to staff via the Vocare intranet.

Role specific requirements are defined in the organisations training needs analysis, supported by regular sharing of information and training.

Mandatory NHS Data-Security Awareness course annually for all staff. Senior and Executive teams complete DPO-delivered training covering their responsibilities.

1.21.3.3-Safe and secure practices for delivering remote and virtual patient contacts

Vocare has extensive experience of remote and video consultations.

a)-Safe

- Patient identity verified and consent gained to access record
- Local clinical guidelines available to all staff via intranet
- System user roles - access to clinical modules defined by skillset [e.g. PaCCS DoS access, electronic prescribing]
- Access to on-shift clinical support through shift leadership and 24/7 Senior GP on call
- Clear protocols for the management of emergencies
- Safeguarding – specific processes for virtual consultations in addition to standard policies.
- Video consultations via secure NHS approved systems [Q-Doctor, Goodsam]
- Risks minimised by independent audits and reviews of remote access services, including clinician call and notes audits, prescribing audits, and productivity and effectiveness monitoring.
- Legislative compliant environment (e.g. health and safety)

b)-Secure

- Access to clinical system via secure login, stronger authentication to minimise risk of unauthorised access.
- Secure network connection [encrypted Virtual Private Network]
- Systems/data access in line with Caldicott Guidelines and Job/Role specific requirements.
- Remote access subject to formally approval - assigned roles and responsibilities for authorising all elements of remote access - business need reviewed before authorised.
- Home working policy - employee self-declaration confirming use of a private, enclosed, undisturbed room where they cannot be overheard.
- Screens and equipment kept out of view.
- Key code entry to remote locations. Supervised third party visitors.
- Virus protection on all system and network components
- Paper light environment.

b.1)-Compliance with policy

- High-level responsibility for managing remote access e.g. monitoring compliance with policy
- Data retention and disposal in accordance with policy.

1.21.3.4-How clinical notes are recorded

All clinical notes are recorded on Adastra EHR. Adastra is delivered using Citrix and all data is stored on secure data-centre servers.

Access is via individual secure login enabling a full audit trail of individual activity to be recorded in the system.

All calls are recorded and audited alongside of clinical records; feedback is provided to staff.