# Remote Working in Primary Care Guidance for GP Practices during COVID-19 Emergency Response

## Appendix to Securing Excellence in Primary Care (GP) Digital Services: The Primary Care (GP) Digital Services (version 4)

## Issued: 30 March 2020

## Contents

# 1 Background

During this exceptional COVID-19 emergency period, significant numbers of general practice staff are unable to work from their normal GP practice base.

This appendix to the GP IT Operating Model sets out additional guidance for CCGs and their IT delivery partners that will support practices with options for remote working. The guidance will remain in force during the COVID-19 emergency response period.

# 2 Remote working options

GP practice staff working away from their practice will need a range of services, depending on their role.

The main options, in order of priority, are:

1. **NHS provided laptop** with all required software necessary for the role together with a token for secure VPN access and, where needed, a smartcard reader. A major effort is underway nationally to secure large numbers of laptops for rapid deployment across the GP practice estate.

2. **Virtualised desktop service.** Some areas have deployed virtualised desktop infrastructure which enables access to critical systems and services from corporate and personal devices. This removes the need to deploy full versions of the applications on the user's device. Where virtualised desktop services are in place, deployment should be maximised as it provides a secure, scalable and cost-effective solution. Several services of this type are at a prototype / pilot stage. Depending on the results of the pilots, some of these services could be ramped up for rapid deployment.

Where options 1 and 2 are not available, the following options should be considered for users that have equipment with the necessary specifications and are able to assess and implement the security requirements.

These products are not strategic but may be used in emergency situations and in the absence of any alternatives or as providers work towards options 1 and 2.

3. **Personal PC / laptop (BYOD)** with all necessary software applications installed and connectivity to HSCN network. A smartcard reader will be necessary for certain applications. This is not an ideal solution as the GP system applications are not optimised for deployment on personal devices. Minimum specification and risks to be considered is set out in Appendix A.

4. **Personal device with desktop sharing over Remote Desktop Protocol (RDP).** This solution involves allowing a remote device to 'take over' a host machine – normally the desktop in the practice office. When the remote device is connected to the host machine, all functions on the host machine can be accessed, including those requiring smartcard access. These solutions can be deployed quickly and at low cost and have been implemented in many practices.

   Key security considerations for using RDP include:

- **Exercising stringent control over machines and smartcards** in the practice. This usually involves securing the offices where the machines are located with a person at the practice having responsibility for ensuring that machines and smartcards are only activated when needed and are switched off when not in use. If the software allows, the host screen should be locked.
- **Data protection impact assessment (DPIA) and clinical risk assessment** must be completed to ensure that the CCG, GP IT delivery partners and GP are aware of the risks and issues with these products.
- **Avoid using "consumer" software and services,** instead use corporately procured solutions (licensed to the practice or CCG as a corporate organisation not the individual) where contracts are in place to protect your organisation and patient data.
- **We must recognise that these systems bypass certain NHS security measures** (smartcard and domain account controls) and to be used with all the above cautions taken on board, if options 1- 3 are not available from the CCG.

## 3 Use of smartcards in remote working environment

To realise full benefits of the clinical systems and national applications, a smartcard is required for each user. Alternative processes are possible if a user does not have access to a smartcard (or smartcard reader). These will depend on the software being used, and the need to access spine services such as SCR, EPS and eRD. Home users should work on the principle of taking the most appropriate decision and if a smartcard related action is required, a member of practice-based staff can complete the process using their smartcard.

## 4 Additional Resources

https://digital.nhs.uk/binaries/content/assets/legacy/pdf/a/3/byod.pdf

https://beta.bma.org.uk/advice-and-support/covid-19/practical-guidance/covid-19-remote-consultations-and-homeworking

## 5 Glossary

BYOD – Bring Your Own Device (i.e. use of personal computer)

DPIA – Data Protection Impact Assessment

HSCN – Health & Social Care Network

RDP – Remote Desktop Protocol

SCR – Summary Care Record

EPS – Electronic Prescription Service

eRD – Electronic Repeat Dispensing

## Appendix A - Minimum Personal Equipment Specification

**Windows PC / Laptop**

- Windows 10 (pro version if possible)
- Windows updates routinely applied
- 8 GB RAM
- 30 GB free disk space
- Hard disk encryption if possible (such as BitLocker, built-in to Windows 10 Professional)
- Screen Resolution 1280 * 1024
- Internet Explorer version 11 (native mode)
- Processor Core i3
- Microsoft Office installed
- Anti-Virus / Anti-Malware Software installed with current active licence and updates (such as Windows Defender, built-in to Windows 10 Professional)
- Broadband connection

**Apple Mac Desktop or MacBook**

These will require Windows emulation software such as VMware Fusion or Parallels Desktop.

**Users will also require**

- Smartcard reader
- Headset and microphone (if VOIP to be provided)
- Clinical System client software
- A HSCN (N3) VPN access token.

**File storage**

Secure arrangements need to be provided for patient identifiable information (not local drive on personal device and not personal or default Microsoft OneDrive or similar storage).

**Risks to be considered when deploying applications on personal devices**

- Personal devices may not have encrypted drives
- Clinical System, Document Management and NHS Mail may cache patient information on local unencrypted drive
- Personal device may be cyber compromised (e.g. virus or malware or unpatched operating system)
- Potential for conflicts with locally installed (personal) software.