Cymorth Llywodraethu Gwybodaeth ar gyfer Gofal Sylfaenol
Information Governance Support for Primary Care
IGDC • DHCW

IG Guidance for Primary Care Services

Remote Working for General Practice Staff; including Working from Home

Introduction

Information Governance is a framework which supports how organisations and individuals manage the way information is handled. It applies to sensitive and personal information of employees, patients, and service users. It is about setting a high standard for the management of all information and giving organisations the tools to achieve that standard.

It is recognised that there is a need for a flexible approach to where, when and how General Practice staff undertake their duties or roles, particularly when working remotely.

Handling confidential information outside of your normal working environment brings risks that must be managed. Examples of remote working include, but are not restricted to:

- Working from home;
- Working whilst travelling on public/shared transport;
- Working from public venues (e.g. coffee shops, hotels etc.);
- Working at other organisations (e.g. NHS, local authority or academic establishments etc.);
- Working abroad.

This guidance aims to support staff whilst working remotely. For this guidance, the term 'staff' includes all health professionals, partners, employees, locums, students, trainees, secondees, volunteers, contracted third parties and any persons undertaking duties on behalf of the Practice.

As a control measure to mitigate risks involved in remote working, no member of staff will work remotely unless they have been authorised to do so by their line manager. Remote working must only be authorised for staff who are up to date with mandatory information governance training.

Whilst working remotely, it is critical for all staff to ensure that confidentiality of any information is maintained, and that Practice property and files are stored securely, protecting

them from loss, destruction or damage and not left in a vulnerable position or open to access by non-authorised persons.

The following guidance will help staff take the necessary precautions against loss and theft and will also reduce the risk of information being disclosed to unauthorised individuals.

This guidance should be read alongside the following policies, along with the relevant organisational procedures:

- All Wales Information Governance Policy for Primary Care Service Providers;
- All Wales Information Security Policy for Primary Care Service Providers;
- All Wales Internet Use Policy for Primary Care Service Providers;
- NHS Wales Email Use Policy for Primary Care Service Providers; and
- NHS Wales Microsoft 365 Acceptable Use Policy for Primary Care Service Providers

Appropriate Equipment

The organisation is responsible for ensuring staff are provided with the appropriate equipment to perform their duties. Where staff require a laptop to perform their work, it should be one which has been supplied, configured, and maintained by Digital Health and Care Wales (DHCW). There are exceptional circumstances to this, see the Use of Own Equipment and GP Remote Desktop Service sections below.

Access must be through a secure connection provided by the organisation, for example via VPN, Soft Token or Multi Factor Authentication (MFA).

Staff must ensure that all software on the device is kept up to date. DHCW will regularly perform updates to DHCW managed equipment, to ensure updates are made promptly. Once available, staff should ensure they regularly connect the device via VPN or directly to the Practice network.

Use of Own Equipment

It is not advisable for staff to use their own personal devices for the management of patient information. However, we appreciate that there may be circumstances when staff are required to work remotely and who will be relying on the use of their own device and access to the network through MFA.

The ICO recommend this approach is captured in an appropriate policy, therefore the GP Practice is encouraged to develop and implement a Bring Your Own Device (BYOD) Policy. See the National Cyber Security Centre (NCSC) website for further guidance.

Where there is no other practical alternative staff should ensure:

- The device is appropriately maintained, and appropriate software updates and patching have been applied;
- The device is not jailbroken or any other tampering that alters the products security;
- The device is appropriately protected with anti-virus products;
- The device is kept secure with strong passwords or bi-metric access controls;
- No personal/confidential data is stored, downloaded or recorded on personal devices;
- Home internet connections are secure (i.e. use a virtual private network (VPN) and avoid using public WIFI.

GP Remote Desktop Service

The Remote Desktop Service has been set up to support GPs and key practice staff who require continued emergency access to their IT systems from home computers. The solution provides a remote connection from a home computer or device to the computer situated in the GP Practice. The anticipated use cases are:

- GP (including locums) has to work from home/outside their normal place of work;
- Other forms of remote working (i.e. VPN via a work laptop/device) are not available;
- Where a 'work' (i.e. based in a practice) PC/laptop is:
    - switched on;
    - connected to the relevant network; and
    - has the relevant software installed.

A GP working remotely will be able to logon to a practice PC remotely via the GP Remote Desktop application using their own computer/device that has the relevant software installed.

A Request Form and User Guide are available for the GP Remote Desktop Service by logging a call with the DHCW Service Desk. Where the use of the service is deemed necessary, staff are responsible for ensuring that guidance provided is adhered to.

Accessing NHS Wales Applications via Multi Factor Authentication (MFA)

Staff accessing NHS Wales applications via MFA must receive line manager approval prior to using personal devices for this purpose. The need for staff to access NHS Wales applications offsite is limited and should only be on a read-only basis. Staff must not:

- save any documents/emails to the device;
- print or download any documents/emails;
- forward any documents/emails from or to non-NHS Wales email addresses.

Security of Equipment and Personal or Confidential Information

Staff are responsible for taking adequate steps to ensure the security of DHCW managed equipment and personal or confidential information when working remotely, including in their home. Staff must not allow any other person, including family members, to use or have access to the laptop or work files.

At the end of the working day documents and devices should be stored securely and not accessible to anyone else, they should not be visible through windows or doors, or in the vicinity of external doors, porches, or outbuildings. Under no circumstances should business sensitive documents or documents containing personal information or managed devices be left in a vehicle overnight.

Staff must consider the confidentiality of their workspace, particularly where their workspace is shared or accessible by others, including family or friends. Staff should be mindful of where

they hold conversations in person or via telephone/MS Teams/video call particularly where staff are discussing personal or confidential information. For example, during a video consultation, staff must ensure the environment is appropriate to guarantee confidentiality. Staff should ensure the laptop screen is positioned where it is less likely to be overseen, if the laptop is left, even for a short time, then it must be screensaver locked using 'Ctrl+Alt+Delete and Enter' or by using the 'Windows Key + L'.

Staff should not attach any personal removable media (i.e. USB memory sticks) to managed equipment, unless authorised to do so. Where staff are authorised to store confidential information on removable media, the device must be encrypted and approved by DHCW.

Staff should take care to ensure that any documents are appropriately backed up, for example saved to OneDrive, SharePoint, or network drive, as appropriate, to ensure business continuity in the event of the device being lost, stolen or malfunctioning. See the below section on Incidents for further information.

Secure Disposal

Staff must ensure that any paper-based documents, including handwritten notes, that are no longer required are appropriately destroyed. For example, using a cross-cut shredder or confidential waste disposal. If staff do not have access to an appropriate shredder at home, the documents must be appropriately stored and brought into the Practice to be shredded or destroyed as confidential waste.

Staff should try to reduce paper-handling and only print documents or work on them outside of the Practice where necessary, as they will be vulnerable to theft or misplacement.

Incidents

Staff are responsible for ensuring any incidents are reported in line with local incident reporting procedures.

In the event a device, including, but not limited to, laptop, VPN token, or removable media is lost or stolen, the organisation must inform the DHCW Service Desk as a matter of urgency.

Where a data breach occurs, the organisation should liaise with their Data Protection Officer (DPO) as soon as possible in order for an assessment of the breach to be made, and investigations started. Where the breach is assessed as being likely to have a high risk to an individual's rights and freedoms, it must be reported to the Information Commissioner's Office within 72 hours of becoming aware of the incident. The ICO website provides a guide which contains further information on data breaches and how they should be handled in line with Article 33 and 34 of the UK GDPR.