|  |  |
| --- | --- |
| OAKLEY HEALTH GROUP | |
| REMOTE WORKING POLICY | |
| REVIEW DATE: | 18.04.2020 |
| REVIEWED BY: | Dr Neil Bhatia |
| NEXT REVIEW: | 01.04.2021 |

This policy covers the information security issues inherent in remote (“home”) working.

There has been a rapid expansion in remote working necessitated by the COVID-19 pandemic.

Accordingly, [a DPIA was undertaken](https://www.dropbox.com/s/cy6qb0w8b43dom7/OHG%20DPIA%20remoteworking.pdf?dl=0) and information security risks and mitigations were identified. These have been listed here and so form this policy.

Information security is:

* the processing of data securely by means of “appropriate technical and organisational measures”
* ensuring the ‘confidentiality, integrity and availability’ of our systems and services and the personal data we process within them

Oakley Health Group places data protection at the heart of our organisation.

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/>

All members of Oakley Health Group that are working from home, or intend to, should read this policy, understand it, and follow the advice therein.

**RISKS IDENTIFIED**

The principle risks associated with home working centre around information security, both paper and digital. Since the ability to remote consult allows all functions of medical care (other than a face-to-face encounter), the *location* of the healthcare worker, whether at home or in any surgery, is irrelevant as long as that member of staff has access to the full GP record.

Whilst it should be made aware to patients that staff will – *like the rest of the country* – be working from home, there is no particular need to indicate to the individual patient being consulted that the GP they are speaking to, for example, is not in surgery but at home. Data protection considerations are not related to the location, but to the *setup and security* that remote working must address.

The information security risks identified are as follows:

1. Risks inherent in the *transportation* of data (paper and digital) from work to home (and vice versa), for the purpose of facilitation remote working. Examples would include printouts of patient records, searches, audits, correspondence from or about patients not yet filed/uploaded to the electronic GP record.  
   Data breaches could occur from loss of paper records and loss of digital media (especially if unencrypted), including the loss of the laptop destined for homeworking use.  
   Security risks from the sending of confidential data by email from and nhs.net account accessible at work to a non nhs.net account (e.g. Gmail) more easily accessible at home.
2. Risks inherent in the *storage* of data whilst at home, again both paper and digital. Where that data is stored, and for how long.  
   Data breaches, or unlawful processing, could occur if data is downloaded from the GP record to “cloud storage” (which may be unbeknown to the user), and which could then be processed, in an unencrypted form, outside of the EU (Dropbox being an example).  
   Data could be inadvertently downloaded to the local hard drive and *not deleted* once there was no further purpose. Local caches can be difficult to find and clear, and files (containing person confidential data) can be downloaded and “lost” simply because the user does not know where downloads are stored.  
   Inadvertent and/or insecure disposal of printed personal data.
3. Risks inherent in the *security considerations* of the home PC or laptop.   
   Failure to install or update antivirus/firewall software, or apply Windows security updates.  
   Failure to change the default password of the home router and/or ensure that home network access is encrypted with at least WPA2.  
   The usage of less well protected email accounts than nhs.net, and the inadvertent opening of emails from unknown sources, malicious links, or downloads of malicious files.  
   Those risks will be amplified if and when access to NHS applications (such as EMIS Web, Docman, iGPR etc.) can occur *without* the need for an N3/HSCN VPN.  
   Inadvertent access by other family members to “shared” drives within the home network, some of which might be temporary storage locations for downloaded patient data.  
   Screens left unlocked, visible, and displaying personal data – failure of password protected screensavers and the usage of the lock screen.  
   Risks inherent in conducting remote consultations at home, where screen, video, and telephone conversations can be overheard by family members.  
   Potential for the loss/theft of laptops – and the risks of a data breach of personal data is stored *unencrypted* on such a device.
4. Risks inherent in the *greatly increased* use of email and texts (which do not afford the user the immediate opportunity to validate the recipient, unlike a telephone call).  
   Accidental disclosure of personal confidential data to the wrong individual because of an incorrect email address or mobile telephone number.
5. Risks inherent in the *greatly increased* use of messaging apps to remain in communication with each other.  
   Accidental disclosure of personal, confidential data onto insecure platforms, or hosts based outside of the EU, such as WhatsApp, when perfectly secure alternatives exist.
6. Risks inherent in the *generation of tasks* – processes that can *only* be done whilst at the surgery (certain referrals, printing of request forms, labelling of specimen containers etc.)  
   The use of “post-it” notes or notebooks to store such “to do” lists.

**MITIGATIONS AGAINST THOSE RISKS**

1) **Transportation/transfer risks**

* Minimise the need to take paper records to and from home.  
  Scan/digitise such records and upload (see below).  
  Ensure all patient correspondence is scanned and uploaded to the electronic record before working from home, so that it is available via EMIS or Docman.

If needed, download the relevant records once home/at work.

* Minimise (ideally obviate) the use of USB drives.  
  Never store personal data on a USB drive unless it is encrypted (at least 128bit AES).  
  Upload personal data to Microsoft One Drive for Business (NHS).  
  Such data does *not* have to be encrypted at source.  
  OHG has undertaken [a risk analysis for NHS OneDrive](https://www.dropbox.com/s/dxdai1urhdrd7wh/NHSOneDriveRiskAssessment.pdf?dl=0).  
  Download the relevant data once at home/work from OneDrive.  
  Delete the data from OneDrive when no longer needed.

Do NOT upload personal data (even if encrypted) to Dropbox or Google Drive.

* Ensure comprehensive security for all paper and digital media during transportation to and from home.  
  Put paper records (if absolutely necessary) in secure storage, such as a locked briefcase.  
  Do not leave laptops in a vehicle, especially where visible from the outside. Lock the laptop in the boot, and do not store the laptop in the vehicle boot overnight.  
  Ensure laptops are stored away from windows and doors when at home.
* Never send yourself personal data from your nhs.net address to a non nhs.net address (e.g. Gmail or Yahoo), and vice versa.  
  Ideally, never send yourself *any* personal data, even from your nhs.net address to your nhs.net address. It is easy to accidentally send that data to a third party, especially where the autofill address option is active.  
  Upload such data to OneDrive (or encrypt it and transfer it to a USB device).

2) **Storage risks**

* Always download, or transfer, personal data from OneDrive, a USB stick, EMIS, or Docman, to your local hard drive – not to folders synchronised with cloud storage (e.g. Dropbox).  
  Know where downloads are put from EMIS, Docman etc., so that you can find them and delete them when no longer required.  
  Set up a universal download folder where any, *and only,*   
  practice-related personal data is always stored.  
  Do not store practice-related confidential data in the same folder as your home-related personal data.
* Regularly check your folder. Delete any downloaded data as soon as it is no longer required. *Permanently* delete it, or “empty” the Recycle Bin immediately to avoid inadvertent ongoing storage of the data on the hard drive.
* Do not print off documents containing personal data if possible.  
  If you do, *shred* that document once no longer required – do not simply put it in the household waste.  
  If you do not have a shredder, securely transport it back to the surgery and then securely dispose of it in the usual ways.  
  Do not leave printed documents lying around at home – keep a “clear desk” policy as you do at work. Young children, in particular, like grabbing pieces of paper, drawing on them, and sending them to teacher/friends.

3) **Home PC/laptop**

* Ideally, the home laptop or PC should be running Windows 10.  
  Windows 7 is no longer being provided with security updates.  
  If at all possible, users would upgrade to Windows 10 as soon as possible (it remains free to upgrade, still, with a Windows 7 licence key).
* Never run a home PC or laptop without up to date, and enabled, antivirus and firewall software. Windows Defender is perfectly acceptable.
* Ensure that your home router’s default password has been changed, and that connections to it are encrypted via at least WPA2.
* Take care not to open emails from unknown senders, click on malicious links, or download infected files, from your personal email accounts.  
  **Don’t click on unfamiliar web links or attachments claiming to give you important COVID-19 updates.**
* Always connect to the N3/HSCN VPN when access to NHS applications is required. Disconnect from the VPN when no longer required.
* Make sure that you do not download personal data from clinical applications to “shared drives” accessible by other family members (e.g. external storage).
* Always lock (Windows key + L) the screen when leaving it unattended. Make sure it is password protected.
* Take care to ensure that your screen is, as much as possible not being overlooked by other family members, or by someone outside of the house (e.g. if your monitor is next to a window). Consider buying a privacy screen if needed.
* When consulting, ensure as much as possible that your telephone and video conversations cannot be overheard or seen. Use headphones and a microphone (so that your voice can be kept quiet). Ideally, other household members should not be able to walk into view of a video consult (i.e. be seen by the patient).
* It is strongly suggested that all laptops are encrypted to avoid a data breach in the event of loss or theft.
* Turn on your laptop, connect to the VPN, and start EMIS Web well in advance of the start of your session.  
  EMIS can take a while to update, and should there be a technical problem you will have time to consider whether travelling to one of the non-patient facing sites is required(with or without the laptop).
* Do not attempt telephone triage, or responding to an e-consult or email, if you have lost the ability to access the full GP record.
* Always use strong passwords. The [NCSC recommends using three random words together as a password](https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0) (eg 'coffeetrainfish' or ‘walltincake’).
* Make sure you use different passwords for different services/accounts. Don’t use the same password for everything.

4) **Increased use of emails/texts**

* Be careful to check the email address and mobile number of patients to avoid sending a text message, or email, to the wrong person.
* Be extremely careful if automatic name checking/autofill is turned on in your email application. It is very easy to accidentally send an email to the wrong person. Consider turning automatic name checking off.
* Be mindful of the amount, and nature, and appropriateness of information that you send via text/email. Sometimes a telephone call is safest.
* If you do email patients, ensure you record the email conversation in the GP record, however you wish to do this. Attach pictures sent by patients (e.g. via AccuRx) into the patient record, for medicolegal purposes.

5) **Messaging**

* Do not use WhatsApp for communicating about individuals, particularly the disclosure of personal data (name, DOB, diagnosis etc.)
* Do not use non nhs.net email where personal data is involved
* Perfectly safe, secure, and effective alternatives exist should there be the need to discuss patients in this way
* Always consider whether telephoning a colleague would be best, especially if there is a level of urgency. If ringing from home, try not to be overheard by other family members.
* Use “Tasks” or “Internal Email” *within* EMIS Web
* Use NHS mail, especially if you need to share documents
* Consider using any of the other secure collaborative mechanisms available e.g. OneDrive for NHS or Microsoft Teams (which has secure messaging built-in).
* Remember that any personal data left within such apps is disclosable under a data subject access request.  
  If no longer required, delete that data, saving any clinical discussion within the respective GP record(s) as indicated.

6) **Tasks**

* Some things might only be possible once back in surgery.
* If so, send yourself an *electronic* reminder to do such activity
* Don’t use post-it notes.
* Don’t use notepads, especially not notepads that double up as shopping lists