NHS Grampian

Information Governance – Data Protection

Working remotely during COVID-19

Many NHS Grampian colleagues are now quite appropriately working from home to help reduce the transmission of COVID-19. This means that patient records or other resources containing health data (such as dictation tapes) need to be taken outside of the direct health care environment so that work can continue. Wherever possible work should be done on NHS Grampian devices, however in the current circumstances we recognise this may not always be achievable. This guidance has been drawn up to support colleagues in working safely from home.

Taking work home – physical records

NHS Grampian has an existing policy which governs the removal of medical information from normal settings and it is applicable in these circumstances.

In particular:

- Removal of information to the home must be authorised as appropriate by an accountable manager;
- The minimum amount of material should be removed to facilitate home working;
- Material should be removed for the shortest time possible from NHSG records stores/secure NHSG offices (so must be returned quickly);
- Material must be held securely in the home environment per Appendix D of the protocol linked above;
- Records or other assets must be tracked to the officer and location where they are being worked on. The accountable manager is responsible for ensuring this.

Securing your workspace

- No access to NHSG information may be provided to anyone who is not a member of NHSG staff.
- Colleagues must be especially careful in domestic settings that no-one can access data inadvertently, for example by reading something over the shoulder, being able to see screens, overhearing conversations and so on. When work is complete it must be stored securely and/or returned to a NHSG site as quickly as possible.

Accessing data using personal devices

- Use NHS Grampian issued and secured devices whenever possible;
- Where data is accessed using a personal computer, you must do so only in your browser. No data may be downloaded, saved, printed etc to your personal device or in your home. You can access NHS Mail, Near Me and Microsoft Teams from your browser and can save files in Teams;
- If you must consult patient data from home it must remain in core systems and be viewed only. It must never be downloaded to personal devices, stored, transmitted, shared or otherwise used in unapproved systems (ie tools or systems that are not provided by eHealth);
- You must not save your NHSG passwords on your devices or using the 'save password' features in browsers;
- If you use your personal telephone to call patients, your 'recent calls' list on your device must be deleted at the end of each day;
- If you are offering virtual appointments via Near Me please have your NHS badge visible;
- To protect your own number you must block your outgoing caller ID (see for example https://bigtechquestion.com/2019/04/17/phones/withhold-mobile-number/);
- Any device accounts used to access NHSG information must be single-user. That means a username and password on your phone, tablet or computer for the account you use for work that is known only to you and is not used by other members of your household;
- All devices used to access NHSG information must be password-protected, encrypted and be running reputable anti-virus software where applicable;

- Do not upload, store or share NHS data via unapproved commercial solutions such as Dropbox, Googledrive, iCloud, iMessage, Zoom, WhatsApp, text messages, FaceTime, Duo etc;
- Make sure your devices have the latest security patches applied;
- Follow normal good security practices (keep up to date on known phishing and other scams, never click on links in emails from unknown sources etc - https://www.ncsc.gov.uk/section/information-for/individuals-families)

Your responsibility

- NHSG staff are required to have a clinical or business reason to consult healthcare data as normal and under no circumstances should they seek access to any person's data, without authorisation. No-one should be accessing information concerning themselves; colleagues; friends; family members; or neighbours. This includes accessing patients who may be affected or diagnosed with COVID-19 without a legitimate clinical or business reason. The response to COVID-19 does not change that requirement. Inappropriate access to information has the same professional regulatory and contractual implications as always;
- If any work materials are lost, accessed inappropriately or their security is compromised in any way, that must be reported as normal via Datix;
- Changes to working patterns such extensive remote working; extensive removal of data from its normal location; new or novel uses of data; the use of new systems; significant changes to how existing systems are used; or the increased availability of data (including to new or additional audiences) in response to COVID-19 must undergo a rapid IG risk assessment. This process documents information risks, their mitigation and the acceptance of senior management for the new, changed or enhanced activity. Please contact gram.infogovernance@nhs.scot.

Some do's and don'ts

Colleagues at NHS Highland have prepared the following tips to help you secure your workspace:

- **Do not** let your screen or paperwork be viewed by others in your household;

- **Do not** let video or audio conferences be seen or heard by others in your household;
- **Do**, if possible, work in an area where you will have total privacy;
- **Do not** include your home location or telephone number on your email signature;
- **Do** be mindful of your own and your family's privacy when on a video conference, for example, do you have family photographs displayed in the background;
- **Do** store any paper and devices securely and out of sight overnight;
- **Do** not be tempted to leave paperwork out on surfaces. If you have access to a locked drawer, it is preferable to lock paperwork away when not being used;
- **Do** ensure that listening devices in your home, such as Alexa, Siri and Google or similar devices are switched off in the area you are working;
- **Do not** leave paperwork or devices overnight in your car.

If you need any further support or advice around data protection or confidentiality, please contact the Data Protection team at - gram.infogovernance@nhs.scot.