Handling Information Securely: A guide for staff in NHSScotland

Having the right information at the right time is vital to patient care and effective service delivery. All staff have a responsibility to handle information securely – whether it relates to patients, employees or business information - according to Board-level and national instructions. This is essential for business continuity, to be on the right side of the law and most importantly to maintain patient and employee trust that personal data is being handled with due care.

The aim of this short guide is to highlight the top ten information security areas that you need to consider and to sign-post where you can go for further help.

1) What information and equipment do I need?

The essential first step, ideally before you even start work in the health board, is to understand what information and computing equipment you actually need to do your job and to agree this with your manager beforehand.

Your Board eHealth team or GP practice manager will issue you with the appropriate computer equipment, and get you started with 'logons' to the network and to a range of systems that hold data or to places that hold the paper records that you need.

Credentials that you are issued with – such as passwords and tokens- are unique to you and must not be shared with anyone or kept with your computer equipment.

As part of your induction you need to learn how to use the ICT tools and the services which run on them.

Access to a service does not always mean you are allowed to access all the data on it. You must not go beyond what permissions have been agreed with your manager. Your access is monitored by audit logs for investigation, and you will need to justify your access to data at all times.

Not all the information you need will be digital, and the same care and access permissions apply to spoken - face-to-face and telephone - and paper information.

If there is a change in job role, then your access permissions must be changed accordingly by agreement with your manager promptly.

2) How do I access information securely on my computer?

You will need to enter your unique credentials that gives you access to services to start accessing information.

For even short periods away, you need to lock the screen.

Usually you will only be able to access the information you need using the official computing equipment that you have been issued with.

Where there are exceptions to this rule, such as email and some Internet-based services, you will need to follow your Board procedures and be careful not to store information locally. Note: patient or employee personal data should never be actually stored on personally-owned computing equipment.

4) How can I share information securely using email?

Email is likely to be your most common tool for sharing written information. Most data breaches can be avoided by taking the following simple steps:

- Never use personal (non-work) email accounts for NHSS business

- Keep to the one patient = one email message rule

- Keep the number of staff circulation lists to a minimum, and in the case of patient groups avoid them altogether.

- switch off the 'auto-population' address tool and manually enter each address or choose from contacts list.

- Before sending personal or other sensitive data to an external non-NHSS email address check whether this is permissible and if it requires additional steps.

- When an email arrives, think! Is this an unexpected mail, is there any possibility that it could be malicious? If in doubt do not open the email/attachment.

5) How can I share information by telephone, text or video?

Fax should no longer be used in NHSS for transmitting any personal or sensitive corporate information.

Board official telephones (fixed, mobile and IP) can be used to share personal sensitive information, as long as there is due regard to people in the vicinity who may over-hear what is being said.

Two-way analogue radios are not suitable for sharing any personal or corporate sensitive data.

Board issued equipment and operating instructions should only be used for video conferencing calls that identify patients.

Use of personally-owned telephones for voice calls or text messages should be avoided for NHSS business, unless absolutely necessary.

6) How can I send paper information?

For routine correspondence to patients, you should use your Board templates which are designed to keep the amount of personal data to an absolute minimum.

If sending health record files externally, these should be double enveloped and sent via a tracked mail service.

If you are considering sending bulk data - such as that relating to more than one patient - then you need to consult your information security manager on the best way of doing this.

7) How can I store information securely?

It is important that you follow Board records management policies and file information in the right place. This may include a particular shared drive, a clinical system or a paper-based filing system.

NHSS information with any identifiable patient information should not be stored on any personally-owned devices or accounts such as mobile phones and computers or personal off-site 'cloud' services.

Any paper-based files that contain patient information can only be held at home on a very temporary basis (e.g. working in community and needing files that day) and not archived at home.

Use of removable media (dongles, USB sticks etc.) should be avoided entirely. If they are to be used in special cases they must only be Board-issued encrypted devices and not for long term storage.

8) How do I access information on the move?

If you are accessing Board information remotely you should not leave your device or paper files unattended and choose an appropriate place to work (i.e. not a busy public place).

When not in use, in transit or at home, ensure that your device is stowed away safely in an appropriate bag. Keep any computer tokens that you need to access the network, separately. Never share your computer equipment or credentials with anyone else and never leave login details with your mobile device.

If you are using Board official equipment such as laptops and smart phones, you may not be able to connect to some Wi-Fi 'hot spots' in hotels, airports etc. because of the technical settings that are designed to keep the data secure.

9) How do I remove the information I no longer need?

You need to be familiar with your Board records policy that outlines where to file all types of information including emails. In the case of formal medical and corporate records the task of bulk deleting needs to follow a formal process.

Where paper-based information does need to be destroyed on an ad-hoc basis, this needs to be carried out in the workplace using designated bagging areas or shredders.

Similarly, if you need to destroy removable media such as CDs, USB sticks or any other computer equipment this needs to be brought to the eHealth team who have special arrangements in place to de-accession and destroy.

10) What should I do if something goes wrong?

An information security incident can be anything that impacts on the confidentiality, integrity or availability of that information (not just losing a device or files). You need to know how to report a concern in the absence of your manager being available.

Where you have been made aware of a security issue via email, text or some other media (or sent some information by mistake) it is important not to compound the issue by re-sending that personal information to others. It is better to phone your Information Governance team and await instructions.

Discretion in regard to patient confidentiality extends beyond the workplace. Official work email addresses should not be used on online social media sites, and there should be no sharing of any information that may identify a patient or employee on public web-sites. Note: all social media sites are considered as public whether or not you have applied 'friends and family' access controls. If you spot something of concern online that relates to patients or impacts on the operations and reputation of your board, it needs to be reported to your information security manager.

If you feel that someone else has accessed your account or your device has been compromised by malware because you have clicked on a link or file you received via email, you need to alert your information security team immediately. They will advise you whether to keep the device running and in a logged in state (which can help to identify an attacker) or to shut it down.

Information security is now a high level corporate concern, and it is important to be able to report with candour (e.g. it may relate to a work colleague). Each Board has a whistle-blowing policy, and there are people outside your immediate team who can help.

Where can I provide help?

[paste here a sticker with Board contact details and online resources]