Updated January 2021

PSNC Briefing 053/17: Ten steps to help improve data and cyber security within your pharmacy

This PSNC Briefing provides community pharmacy contractors with ten suggested steps to help improve data and cyber security for their pharmacy business.

Background

All pharmacies that previously had access to the NHS National Network (N3) have now been connected to the new Health and Social Care Network (HSCN) – see **PSNC Briefing: How to get more out of your connection - an N3 & HSCN update**. HSCN enables access to the Electronic Prescription Service (**EPS**), the central NHS **Spine** and other NHS IT resources. Just like with past N3 usage, whilst using HSCN and the other NHS IT resources, you should take steps to safeguard your data, systems and electronic devices.

With the continual threat of **cyber attacks**, and the expansion of healthcare services being offered in the community, the **National Data Guardian (NDG)** recommends that healthcare data security standards continue to be reinforced. Contractors and their system suppliers should consider good practices such as those outlined below.[1]

Ten steps to help improve data and cyber security

1. Build awareness in the pharmacy team

- Adopt data and cyber security **template policies** for your pharmacy that explain how to safely use your pharmacy's systems and devices.
- Include discussion of such policies within routine staff training sessions.
- Maintain awareness of cyber risks, e.g. staff should be made aware of the risks from scam, faked or 'phishing' (information-seeking) emails, and be wary of clicking on internet links within emails.
- Make use of online cyber security **training opportunities**.

2. Assess your protections

- Aside from the annual completion of the **Data Security and Protection Toolkit**, contractors could consider further assessments, e.g. the use of self-assessment tools or checklists, or an evaluation of cyber security by a third-party expert. Your system supplier may also publish or share information about any third-party evaluations they have had undertaken on their IT systems.
- Check whether your pharmacy follows **best practice in managing data** drawn from the Information Commissioner's Office (ICO) community pharmacy data-usage study.

[1] NDG also acknowledges that the duty to share information can be as important as the duty to protect patient confidentiality: "Health and social care professionals should have the confidence to share information in the best interests of their patients".

info@psnc.org.uk psnc.org.uk 0203 1220 810

3. Reduce malware risks

- Establish anti-malware defences and policies across your pharmacy business. Your system supplier or IT department may look after this if you have 'managed service' arrangements. Also, it is beneficial if:
  a. software updates are applied automatically; and
  b. machines that mistakenly miss updates can be automatically identified so that the auto-update feature can be switched back on.

4. Consider business continuity

- Familiarise yourself with the process for reverting your pharmacy system to the most recent backup in case of a local system crash.
- Review IT business contingency guidance and the policies you have developed and the planning you have undertaken to support business continuity if an issue occurs.

5. Develop a mobile device working policy

- Consider developing a pharmacy policy for using mobile devices in a work capacity. This policy may include the mandatory use of passcodes, and the ability to remotely wipe data from devices in the event of theft. Your policy will become particularly important if you start to use HSCN-connected mobile devices. The policy should explain how to protect data whether staff are using a mobile device at home or on the move.
- Consider encrypting laptops and mobile devices – for further information speak to your IT system supplier.

6. Manage user account rights

- Limit the number of user accounts which have additional administrative rights which could be used to accidentally install malware. If your system supplier or IT department provides a 'managed service', they will be able to set this up for you.
- Note that The National Cyber Security Centre (NCSC) now recommend organisations do not force regular password expiry. NCSC explain this reduces the those vulnerabilities associated with regularly expiring passwords (described within their password guidance) while doing little to increase the risk of long-term password exploitation. Consider authentication models for signing into your systems.

7. Monitor your network and systems

- Monitor systems and logs for unusual activity that might pre-emptively indicate an attack on your system.
- Monitor network security. NCSC have published network security guidance.
  If your system supplier or IT department provides a 'managed service', they will be able to set this up for you.

8. Continue to process sensitive data carefully

Consider the methods you use to communicate sensitive information:

- Use NHSmail safely, e.g. patient data can be communicated securely when both sender and recipient are using an NHSmail account. Check that the recipient is prepared to accept the information by email, and that the mail address auto-complete feature has not led to the incorrect email address being selected in error. Read about PSNC's practical considerations relating to NHSmail governance.
- Fax machines should only be used to send sensitive data as a very last resort and, when used, staff should consider local "Safe Haven" procedures. Fax numbers should be checked and verified before confidential information is sent to them. There remain goals to completely remove faxes from health and care.

- Sensitive data should be sent electronically and only with appropriate encryption levels. NCSC have issued **data transmission guidance**.

9. Develop a removal media usage policy

- Consider developing a **policy to control all access to removable media** (e.g. the use of USB sticks, or DVDs which contain pharmacy data). NCSC's **removable media guidance** highlights risks with USB usage, e.g. loss of information if the USB stick is lost, and risks if any sensitive data could be extracted by others. There are also risks with an infected USB stick introducing malware to the pharmacy network. NCSC recommend that USB sticks are not used frequently because of such security risks.
- Where USB stick usage is unavoidable for the transfer of sensitive data, pharmacy staff should consider the use of encrypted USB sticks to reduce risk.

10. Use secure and standard system settings

- Strive to use standard and secure system and internet browser settings but avoid upgrading software without authorisation from your IT helpdesk or system supplier.

Note: Your IT helpdesk should be familiar with the range of standard system settings which ought to be used by pharmacy systems and any NHS and clinical applications. These include specific Windows operating systems, internet browsers, and Java (a commonly used computing programming language). These are outlined within NHS Digital's Warranted Environment Specification (**WES**) document. Usually your IT or supplier helpdesk will help to ensure your pharmacy's settings remain in-line with the expected settings.

As more devices become connected to pharmacy networks, it becomes increasingly important that all devices being used are secured and do not provide an easy back-door for a cyber-attack.

Frequently asked questions

Q. How do I maintain security for data that I'm required to send elsewhere?

Sensitive data from the pharmacy should only be shared with those trusted organisations which require such information. For example, EPS prescription data must be sent to NHS Digital's Spine by pharmacy contractors. In some cases, explicit patient consent may be required for the transmission of data. Organisations which receive pharmacy information also become 'data handlers' with their own data protection responsibilities.

Q. I've heard there are issues with continuing to use old versions of Windows – why is that?

Community Pharmacy IT Group's **Windows guidance** explains, older versions of Windows no longer receive free support. Non-supported operating systems do not receive security patching and updates.

If you cannot yet upgrade there are some mitigations e.g. use of compatibility wizards within a newer version of Windows so such software can continue to be used, avoiding the use of an internet browser and isolating the machine from the rest of the network. Your IT helpdesk may also help with applying security patches, maintaining a system inventory of machines, and defining a baseline build for all devices.

Note: These ten steps above are loosely based on NCSC's generic **ten steps to cybersecurity**.

Read more about data and cybersecurity at: **psnc.org.uk/ds**, **psnc.org.uk/cybersecurity** and HSCN at: **psnc.org.uk/hscn**. The **NCSC website** also has a range of associated guidance. If you have queries on this PSNC Briefing or you require more information please contact **Daniel Ah-Thion, Community Pharmacy IT Lead**.