Pharmacy data security and IG training factsheet

DSPTK pharmacy policies

***About the use of this document and related resources**: This data security document assists the pharmacy's aligment with the Data Security and Protection Toolkit (DSPTK). Related pharmacy policies are at PSNC's data security templates webpage.*

New staff should receive induction training about pharmacy data security. All staff should also receive refresher training at least annually. This training factsheet provides a top-level refresher of some key training areas and helps guide staff as to where more guidance is available from.

What is data security and IG?

These rules and procedures the Information Commissioner required are what we refer to as data security and IG, which is to do with the way organisations process or handle information about people who use their services and about the organisation's employees. IG includes aspects of the data protection laws such as the Data Protection Act 2018, the Freedom of Information Act 2000 and the common law duty of confidence. It also incorporates guidance from central government, for example, the codes of practice on confidentiality, records management, and information security published by the Department of Health; and the NHS Care Record Guarantee for England published by the National data security and IG Board for Health and Social Care.

IG is particularly concerned with personal and sensitive personal information, but it also includes commercially sensitive information about the pharmacy, which might also require protection.

What does this mean for me?

As part of your job you are required to:

- Know how to safely and appropriately share information.
- Follow procedures to make sure that sensitive and confidential information is properly protected. Failure to follow these procedures may result in disciplinary action.
- Immediately report to the IG lead any concerns or data security incidents.

If you feel you need more training on information sharing, please speak to senior colleagues.

What kind of information must be kept confidential?

At your job, you might have access to lots of different types of confidential information such as: medical or care records, payroll details, staff sickness, personal information and many others.

You can gain access to this information in lots of ways: through email, fax, computer files, paper records, and even through a conversation – either on the phone or in person. Even confidential information can be shared with the right people. For example, you should share information about the people you care for with other health and care professionals if it is necessary for their care.

How do we protect information?

We can divide security measures into three groups. The table below provides some examples.

Physical measures	People measures	Electronic / information measures
Lockable doors and cabinets	Confidentiality & Security Training	Passwords
Intruder Alarms	Identity Checks	Encryption, Secure email, Tracked post
CCTV	Character References	Secured IT networks
Walls, Fences and Gates	Vetting	Policies, procedures
Soundproofed consultation areas	Lone Worker Training	Electronic Audit Trails
Panic Alarms	Security Staff	Incident Reporting Process

Ensuring good information security

There are many ways to ensure good information security. You could work with your data security and IG lead to think about the measures you could take to improve. Some examples of measures that can be taken to protect information are:

- **Protecting paper records/prescriptions:** Don't leave paper records or prescriptions lying around; lock them away when they're not being used.
- **Protecting electronic records:** Use a password-protected screensaver to prevent unauthorised access to electronic records if you have to leave your computer unattended. Log out of your computer after each day.
- **Passwords:** Don't reuse passwords. Choose good passwords e.g. use of three random words is recommended as a good method by National Cyber Security Centre (NCSC). Keep passwords secret and safe. NCSC also recommends you may write them and keep them within a secure location e.g. a safe.
- **Avoid inappropriate disclosures of information:** Make sure you don't discuss sensitive information in inappropriate venues, e.g. in public areas of the pharmacy. When dispensing prescriptions ask patients to confirm personal information to you rather than you reading their details out loud.
- **Ensure the pharmacy building is secure:** Don't leave key coded doors propped open. If you're the last to leave the pharmacy at the end of the working day, make sure windows and doors are locked. If there is a burglar alarm make sure it is turned on.
- **Seek advice from your IG lead:** Make sure you know who is responsible for IG in your pharmacy and ensure that you seek his/her advice on information governance issues.
- **Follow pharmacy IG policies and procedures:** As part of the NHS IG requirements, all pharmacies will need to put in place policies and procedures to support the secure handling of information. If you are not clear, seek advice from your IG lead on what procedures are in place in your pharmacy.
- **Report incidents:** If you discover an actual or potential breach of information security, such as missing, lost, damaged or stolen information and equipment make sure you report to the person responsible for IG issues in your pharmacy.
- **Portable equipment:** Look after portable equipment such as laptops, PDAs and memory sticks. If you're travelling with them ensure you keep them within your sight at all times. Do not write your password on the device.
- **Know where the hard copy suppliers contact info is** in case of outage e.g. internet, clinical system or power.
- **Removable disks:** Only transfer personal information to removable media such as CDs, DVDs and floppy disks if you have been authorised to do so. Unauthorised access to the information should be prevented by the use of encryption.
- **Mobile device and public WiFi:** The pharmacy should use a mobile device and 'bring your own device' policy and staff should be aware that access of sensitive work content over public WiFi hotspots is not appropriate because of the security limitations.
- **Consider Multi Factor Authentication (MFA)** if needed where this is an option and require an added security later. Some pharmacy software will only run with your main pharmacy system.
- **Keep your devices and your software up to date** with the latest patches/updates with support of your IT support.
- **Contact your** local Smartcard Registration Authority (RA) if: you find a personal Smartcard and can't confirm the owner; if not all staff processing data have Smartcards yet; or if staff need adjustment to their card so it works at multi pharmacy sites.
- **Email scams**: Be careful of suspicious links/attachments, avoid clicking on these. Seek support where needed.

Further pharmacy data security training materials

Additional data security training materials are available, such as:

- materials at psnc.org.uk/dstraining;
- DSPTK Template series doc 03B Introduction training;
- GDPR guidance for Community Pharmacy (short version) (Part 2) training booklet for staff;
- GDPR Guidance for Community Pharmacy (Part 1) for pharmacy IG leads.

Non pharmacy specific training includes:

- NHS Digital Online IG Training Tool "Data Security Awareness Level 1.

This data security document assists the pharmacy's aligment with the Data Security and Protection Toolkit (DSPTK). Related pharmacy policies and more can be found at:

- *psnc.org.uk/ds; psnc.org.uk/dsptk; and*
- *psnc.org.uk/dstemplates.*

Pharmacy contractors with queries about the original template or questions about DSPTK may contact it@psnc.org.uk.
This document is based on a template updated during: Feb 2021