Pharmacy data security and IG training (for induction or refreshment)	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 once per year. This training document is intended to assist with your pharmacy data security training.

Introduction

To ensure compliance with the law and NHS requirements, all staff working in pharmacies that have access to personal information about patients must be appropriately informed of their legal responsibility to keep the information confidential and secure and the ways in which they can do this. Confidentiality and information security are part of the practice known as 'data security and information governance (IG)'. By reading this booklet, you will have learnt what data security and IG is and why it is important for you, your workplace and your patients.

This document includes a number of case studies. Using the knowledge you will gain from reading this guidance, you should be able to answer the questions to test your understanding.

Learning Objectives

After reading this document you should be able to understand:
- what we mean by data security and IG;
- why data security / IG is important;
- what information is confidential;
- what information is personal;
- what information is sensitive personal;
- how to protect confidential, personal and sensitive information; and
- the importance of accurate and up to date information.

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, General Data Protection Regulation (GDPR), 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 central bodies such as Department of 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.

When organisations put IG rules and procedures in place, staff members (including employees, locums, students, etc) need to follow them. This will ensure that everyone, including patients, can be more confident that information is:

- properly protected;
- only shared when it is right and proper to do so;
- accurate and up to date; and
- available when and where it is needed.

Ultimately, it means that your pharmacy will be able to deliver the best possible service to your patients, with reduced risk of reputation damage (or the need to pay a fine) for breach of confidentiality.

Why is data security and IG important?

IG rules and procedures enable us to make sure that we provide a confidential service and that patients can continue to trust us to look after their information.

A Confidential Service: Patient information is confidential. There can be no truly confidential service unless everyone who works in or with the NHS knows what information is 'confidential' and how to keep it confidential. We all need to make sure information is kept secure and report incidents if it goes wrong. How else will we learn and get better?

Headline News!

The Information Commissioner's Office (ICO) is responsible for regulating and enforcing the access to and use of personal information. By the end of 2020, the Information Commissioner's website contained reports of thousands of patients being affected by data breaches involving NHS organisations that ranged from GP practices to large teaching hospitals. The Commissioner has instructed the NHS collectively to make sure that there are strong rules and procedures in place to prevent data being lost, misplaced or stolen. Enforcement action has been taken against the individual organisations that have had data breaches requiring them to take specific steps to ensure personal data is protected. If any organisation fails to carry out the Commissioner's instruction it is at risk of being prosecuted and fined a large amount of money that could otherwise be spent on patient care.

Back in September 2009, the first community pharmacy was singled out by the Information Commissioner for attention.

From these real life occurrences you can see that not only have patients been subjected to a breach of their confidentiality, they have also been put at risk of loss of NHS services if organisations have to make savings due to the need to pay a large fine for failure to improve their information handling procedures.

Every one of us must contribute. No matter how often or how rarely you have contact with patients or information about patients you should report any problems that you see. If problems aren't recognised, they will not be reported and are in danger of becoming accepted working practice.

A confidential service means all organisations and employees providing care or treatment to patients have a duty of confidentiality – not just the members of the pharmacy staff that patients have direct contact with.

Patient Trust: Patients trust the NHS and your pharmacy, to record information about their health, look after the information securely and only give it to those who need to see it.

"*Patient Information Held Securely!*" is not a headline you will see in a national newspaper because patients expect (and it is enforced by law) that their information will be properly looked after. Everyone providing services to patients is in a position of public trust – and everyone has to work hard to avoid failures that not only could cause significant patient embarrassment or distress but could become the next day's headline and lead to fines against the pharmacy or staff.

To keep patient information confidential, secure, accurate and up to date - **everyone** must help.

National Data Guardian's Data security standards

The National Data Guardian (NDG) for Health and Social Care is an independent, non-regulatory, advice giving body that has set out key data security standards for health and care. These are set out below.

Data Security Standard 1: All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form.

Data Security Standard 2: All staff must understand their responsibilities under the Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

Data Security Standard 3: All staff complete annual security training that is followed by a test, which can be re-taken unlimited times but which must ultimately be passed. Staff are supported by their organisation in understanding data security and in passing the test. The training includes a number of realistic and relevant case studies.

Data Security Standard 4: Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

Data Security Standard 5: Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

Past security breaches and near misses are recorded and used to inform periodic workshops to identify and manage problem processes. User representation is crucial. This should be a candid look at where high risk behaviours are most commonly seen, followed by actions to address these issues while not making life more painful for users (as pain will often be the root cause of an insecure workaround). If security feels like a hassle, it's not being done properly.

Data Security Standard 6: Cyber-attacks against services are identified and resisted. Staff are trained in how to report an incident (to the IG lead). Basic safeguards are in place to prevent users from unsafe internet use e.g. Anti-virus, anti-spam filters and basic firewall protections are deployed to protect users from basic internet-borne threats.

Data Security Standard 7: A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

Data Security Standard 8: No unsupported operating systems, software or internet browsers are used within the IT estate [without mitigations].

Data Security Standard 9: A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework. This is reviewed at least annually. NHS Digital Data Security Centre assists risk owners in understanding which national frameworks do what, and which components are intended to achieve which outcomes.

Security standard nine expands the organisations cyber security framework to detail the granular technical controls expected to meet mandated MCSS and NIS requirements. For example, DSPT assertion 9.3.6 mandates that the organisation is protecting data in transit (including email) using well configured TLS 1.2 or better.

There is a clear understanding that organisations can tackle the NDG Standards in whichever order they choose, and that the emphasis is on progress from their own starting points.

Data Security Standard 10: IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the Data Security Standards.

What information is confidential, personal and sensitive?

Three common classifications of information are, 'Confidential', 'Personal' and 'Sensitive Personal'

Confidential information

Information is considered confidential if it meets three simple conditions:
1. it is private information about a person;
2. it was provided to someone who has a duty of confidence (e.g. the pharmacist and other members of the pharmacy team); and
3. you expect it to be used in confidence.

All information provided by patients to pharmacies about their medical conditions including prescription information is therefore confidential.

Personal information

Personal information is information that identifies an individual. The most common are obvious things like:
- name;
- address;
- date of birth;
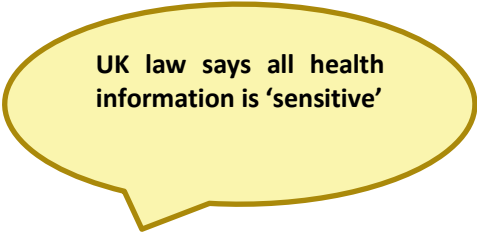- home telephone number; and
- postcode.

It also includes combinations of these that can be put together to identify an individual.

Sensitive personal information

Sensitive Personal Information is information that is more likely to cause a person damage or distress if the information was misused such as:
- racial or ethnic origin;
- political opinions;
- religious beliefs;
- trade union membership;
- physical or mental health or condition;
- sexual life; and
- criminal record.

There is other information that could also be included here. For example if an individual's bank details, salary, credit card details, or National Insurance Number ended up in the wrong hands, it could lead to someone stealing that individual's identity, running up bills in their name and ruining their credit rating. Certainly this would fall into the 'sensitive' category (and whoever failed to look after the information may end up in court).

> **UK law says all health information is 'sensitive'**

The law does not make a judgement on the perceived sensitivity of health information, that is, in the eyes of the law an 'ingrown toenail' is in the same category as 'schizophrenia'.

Why do we protect information?

There is no choice about protecting personal information. UK and European laws, such as the common law duty of confidence and the General Data Protection Regulation demand it.

The common law duty of confidence: the common law requires that normally when confidential, personal or sensitive information is given in confidence to a member of the pharmacy staff it is not shared with anyone else unless the patient gives his or her permission.

Data protection legislation: sets out how organisations should 'process' or handle personal data and provides people with rights regarding data held about them. It applies to all personal data, not just to health and social care records. The same rules apply to information your employer holds about you, for example in finance, personnel and occupational health records. ICO and GDPR set out **key principles**
- lawfulness, fairness and transparency;
- purpose limitation;
- data minimisation;
- accuracy;
- storage limitation;
- integrity and confidentiality (security); and
- accountability.

RPS Code of Ethics and Professional Standards: The Royal Pharmaceutical Society of Great Britain's Code of Ethics also requires that all pharmacists and registered technicians take all reasonable steps to prevent accidental disclosure or unauthorised access to confidential information and ensure that confidential information is not disclosed without consent, apart from where permitted to do so by the law or in exceptional circumstances. Failure to adhere to these standards could form the basis of a complaint of professional misconduct.

Case Study 1 of 3 for trainees: Celebrity spotted. Answer the questions:

A famous rock star visits a pharmacy to pick up a prescription.

As well as purchasing his Nicorette gum, they also collect a bottle of Methadone on prescription. Whilst it was well known that the individual smoked, their opiate addiction was not common knowledge.

The member of staff who served the individual tells other members of the team and they read the rock star's patient medication record. It appears that the rock star has been prescribed methadone for a number of years. That evening on the phone to a friend, one of the staff says, "You'll never guess who was in our pharmacy today" and also mentions the individual's smoking and history of opiate addition.

The next morning, the story is published on the front page of a national newspaper and the rock star's lawyer threatens to sue the pharmacy unless all the culprits are found and disciplined.

The pharmacy carries out an internal investigation to try to identify who disclosed and who viewed the Patient Medication Record.

> **Question:** *Which of the following actions were the staff members NOT justified in carrying out?*

- Viewing the patient's Patient Medical Record
- Sharing information relating to the patient's prescription
- Disclosing information relating to the patient's past prescription history

Check your answers at the end of this document.

How do we protect information?

Information is protected by ensuring that confidentiality is maintained and that security measures are in place to protect against loss, damage or destruction of the information. If confidentiality is more about why we should protect information, the focus for security is on the how, for example, using passwords, locks and security passes.

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

Our security is only as strong as our weakest link – so carrying out assessments of **physical security** measures already in place is vital to identify weak areas (e.g. door locks) that can be strengthened, and areas where security measures are adequate. The measures in place will vary depending on what risks are present - a bit like fitting window locks at your home if you live in an area prone to burglaries, even though people living elsewhere might not need to fit locks.

People measures are central to good (or bad) security – so we have put them in the centre column. The measures overlap to create a 'secure environment'. But security measures are of little or no use if we don't all know which affect us, or if we can't or don't know how to use them.

Probably the worst position for any organisation is not knowing that a risk exists – or that security measures are not working (and not being reported) – for example not knowing that a neighbour was burgled and the same happening to you the next week. It is important that all staff report incidents to the pharmacy's IG lead. If we don't report incidents the necessary measures are often put in place after the incident has happened more than once.

UK law says personal information must be protected

Finally, it is important that the information we use is a reliable presentation of what was recorded, particularly personal information as this is used to provide care and treatment. Implementing appropriate electronic information security measures helps to ensure that information created or used is accurate, complete and not tampered with (e.g. using electronic audit trails to monitor access to records). The measures put in place must also ensure those authorised to use information have access to it where and when it's needed.

Ensuring good data and cyber security (including top tips)

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. Return paper records to the correct storage area when no longer required so that they are available if needed by someone else.
- **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, lock windows and doors. If there is a burglar alarm, turn it 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.
- **Know where the hard copy suppliers contact info is** in case of outage e.g. internet, clinical system or power.
- **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.
- **Removable disks:** Only transfer personal info to removable media such as disks and external hard drives if you have been authorised. Unauthorised access to the information should be prevented by the use of encryption.
- **Mobile devices 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 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.

Case Study 2 of 3 for trainees: Patient mix-up

John Smith walks into a chemist and asks whether his prescription is ready for collection. The pharmacy has been very busy and the dispensing assistant hands over a prescription bag labelled for "Mr. John Smith". Two hours later, another John Smith comes to collect his prescription, and it becomes clear that the wrong prescription items have been given to the original John Smith. Both patients are extremely angry and the dispensary is left in a difficult situation.

➢ **Question:** What could have been done to avoid this situation?
Check your answers at the end of this document.

How can you ensure information is accurate and up to date?

It is important that when a patient medication record is created it is accurate, accessible, and complete. This will ensure that the most up-to-date and relevant information is available at the point of need (for example, when providing a vaccine or prescription intervention).

Accurate, accessible and complete records will also protect the legal and other rights of the pharmacy, its patients, staff and any other people affected by its actions, and provide authentication of the records so that, if needed, the evidence obtained from them is shown to be believable and reliable.

Pharmacists are required by the RPSGB "Code of Ethics for Pharmacists and Pharmacy Technicians" to make and keep accurate and complete patient records. In addition, pharmacy record keeping guidance is at: **psnc.org.uk/recordkeeping**. NHS Transformation Directorate set out some recommended minimum retention periods within their **Records Management Code of Practice for Health and Social Care**. The Specialist Pharmacy Service (SPS, **sps.nhs.uk**) also recommend minimum retention periods for many types of pharmacy data.

On a day-to-day basis, you can ensure that information in patient records is kept up to date by:
- Regularly checking with patients whether any of their information has changed. For example, by confirming they still live at the same address when handing out a prescription.
- Accurately recording the patient information you obtain.
- If it is a hand-written record - making sure that others can read your writing.
- Updating a record at the time you receive the information or as soon as possible afterwards.

Case Study 3 of 3 for trainees: Delayed treatment

You briefly looked at the data protection principles earlier, but here's a recap. Have a read of them then look at the scenario below and see whether you can decide which of the Principles, summarised below, have been breached.
- lawfulness, fairness and transparency;
- purpose limitation;
- data minimisation;
- accuracy;
- storage limitation;
- integrity and confidentiality (security); and
- accountability.

Steven Smith attends his local pharmacy and the pharmacist provides a medicines service with him. Steven is told that he will be sent a reminder for a follow up in a year's time.

Unfortunately, despite telling the pharmacy during his last visit, Steven's address on the system has not been updated since his family moved to a new house a few years ago. As a result, appointment reminders sent by the pharmacy go astray, and when Steven "Did Not Attend" on three occasions the pharmacy assumed that he no longer wanted the service and removed him from the mailing list. Steven is extremely disappointed to discover that the requests were being sent to an old address and makes a complaint to the pharmacy.

> **Question: Which Principle do you think has been breached?**
> - data minimisation;
> - accuracy; or
> - integrity and confidentiality (security);

Check your answers at the end of this document.

Continuity and contacts if something goes wrong

All staff should become aware of who to contact in case of an emergency such as the loss of power, internet or the Patient Medical Record (PMR) system. In some cases digital processes may need to revert to paper causing extra workload pressures during the incident and after it.

Some considerations: Are the contact details of key suppliers available in hard copy format within the pharmacy in case of loss to the computer? E.g. on the wall or listed within a hard copy of the business continuity plan?

Pharmacy contractor business continuity guidance is available at **/bcp**. This includes a Business Continuity Plan template which can be used to enter in key contact details: i.e. the electricity supplier, the internet supplier, the **Patient Medical Record (PMR) supplier** and so on. If you are unsure of where the key contacts information is stored, then check with the data security lead of the pharmacy.

Declaration of Completion of Training

Once you have completed this training, sign the declaration below:

Staff Member's Name	Signature (electronic* or ink)	Date

*Note: Email confirmation that you and colleagues have worked through this training is fine as an alternative to an electronic or ink signature. Your employer may then file the email electronically as confirmations of your refresher training.

Know your IG lead: If you have any concerns about IG in your pharmacy or questions about the processes in place in the pharmacy to protect confidentiality, talk to the person responsible for IG issues or the pharmacist.

The pharmacy IG lead is …………………………………………………………………..

Case Study Answers

Case Study 1:
Answer: The employees had no justified purpose for carrying out ANY of these actions. The scenario leads to the need to discipline staff, loss of reputation for the pharmacy and a risk (to the pharmacy and the staff members) of being sued by the patient and prosecuted by the Information Commissioner.

The duty to maintain confidentiality is part of the duty of care to the patient. It is also a fundamental part of the contract of employment and the Royal Pharmaceutical Society Code of Ethics for Pharmacists and Pharmacy Technicians. The rock star's lawyer is also free to make a complaint to the RPS.

Case Study 2:
Answer: This situation could have avoided if routine checks had been performed, for example asking the patient to confirm the first line of their address or their date of birth.

Although it can be easy to forget to perform checks like this on a routine basis, it is important that they are carried out to prevent being put into difficult situations such as this.

Case Study 3:
The correct answer is "accuracy." The information in Steven's record was not kept up to date. This meant that his medicines service appointment was delayed. Due to the pharmacy error, Steven had to wait longer for the service.

Situations such as this can affect the reputation of the pharmacy and potentially the patient's health. Steven will be less confident that the staff know what they are doing and will feel annoyed or angry that his appointment was delayed unnecessarily. The pharmacy should put a process in place to check patient details and ensure that when they receive latest information such as a change of address; all relevant systems are updated as soon as possible.

CPD training
For any pharmacist, understanding IG will be relevant CPD. Why not make a record in your CPD Plan & Record file or online at the **General Pharmaceutical Council (GPhC) website**.

Further pharmacy data security training materials
Additional or alternative data security training materials are available, such as:
- materials at **psnc.org.uk/dstraining**;
- **DSPTK Template series doc 03C Introduction training two page factsheet**;
- **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 alignment 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.
Document updated: April 2022

Notes: The contents within this document were produced by PSNC and RPS with support from Department of Health and Social Care and NHS Digital. The contents have been further updated to incorporate recent changes.