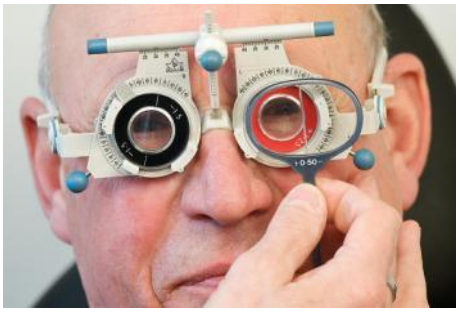
Information Governance Training Booklet for Optical Practice Staff



Optical Confederation
The voice of UK optics

AOP
ASSOCIATION OF OPTOMETRISTS

abdo
Association of British Dispensing Opticians

FODO
FEDERATION OF (OPHTHALMIC AND DISPENSING) OPTICIANS

LOC SUPPORT UNIT
SUPPORT FOR PRIMARY EYE CARE DEVELOPMENT

Introduction

To ensure compliance with the law and NHS requirements, all staff working in optical practice 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 'Information Governance'.

By reading this booklet, you will have met the first stage of this requirement by understanding what is meant by Information Governance and why it is important for you, your workplace and your patients.

This booklet 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 booklet you should be able to:

- ✓ Understand what we mean by Information Governance
- ✓ Understand why Information Governance is important
- ✓ Understand what information is confidential
- ✓ Understand what information is personal
- ✓ Understand what information is sensitive personal
- ✓ Understand how to protect confidential, personal and sensitive information
- ✓ Recognise the importance of accurate and up to date information

What is Information Governance?

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 2009, 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.

The rules and procedures required by the Information Commissioner are what is referred to as Information Governance. These relate to the way that organisations process or handle information about people. Information Governance includes aspects of the law such as the Data Protection Act 1998, the Freedom of Information Act 2000 and the common law of 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 Information Governance Board for Health and Social Care.

Information Governance is particularly concerned with personal and sensitive personal information, but it also includes commercially sensitive information about the optical practice, which may also require protection.

When organisations put Information Governance 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
- Available when and where it is needed

Ultimately, it means that your optical practice 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 Information Governance important?

Information Governance rules and procedures enables 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?

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 optical staff that the patients have direct contact with.

Patient Trust: Patients trust the NHS and your optical practice 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 that their information will be properly looked after and this is enforced by the law. 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 optical practice or staff.

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

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 proved to someone who has a duty of confidence (e.g. the optometrist and other members of the optical team)
3. You expect it to be used in confidence

Information provided by patients to optical practice about their medical conditions including prescription information and family history is therefore confidential.

Personal Information

Personal information is information that identifies an individual, for example:

- Name
- Address
- Date of birth
- Home telephone number
- Postcode

It also includes combinations of these that can be put together to identify and 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
- 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 bill 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 Data Protection Act 1998 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 optician's staff it is not shared with anyone unless the patients gives his or her permission.

The Data Protection Act 1998: 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. The Act contains eight principles that require that organisations are fair and open when they handle personal information. Principles 1, 2 and 7 are the most relevant in terms of protecting information but all are shown here for completeness.

Principle 1: Personal data shall be processed fairly and lawfully.

Principle 2: Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in a manner incompatible with that purpose or those purposes.

Principle 3: Personal data shall be adequate, relevant and not excessive for its purposes(s).

Principle 4: Personal data shall be accurate and where necessary kept up to date.

Principle 5: Personal data shall not be kept for longer than is necessary for its purpose(s).

Principle 6: Personal data shall be processed in accordance with the rights of data subjects under the Act.

Principle 7: Appropriate technical and organisational measures shall be taken against unauthorised of unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Principle 8: Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

College of Optometrists Code of Ethics and Guidance for Professional Standards: The College of Optometrists' Code of Ethics also requires that all optometrists and optical staff 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

A famous pop star visits an optical practice for a sight test. Intrigued and excited by the visit a member of staff reads the pop star's record sight test record without any clinical need to do so, under general health they see that the pop star is taking an anti-depressant and under family history it is recorded "unknown – patient adopted". It is generally believed that the pop star's parents are two other famous musicians.

The staff member then shares this "exciting gossip" with a friend.

A few days later the story is published in a national newspaper and lawyers for the pop star and their parents threaten to sue the practice unless the culprits are found and disciplined.

The practice carries out an internal investigation to try and identify which staff not involved in the patient's care viewed the record and who disclosed the information.

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

- Viewing the patient's records.
- Sharing information relating to the patient's general health.
- Disclosing information relating to the patient's family history.

Check your answers on page 16.

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	Confidential & 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 upon what the risks are to the optical practice – similar to fitting window locks at 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 affects 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 to report incidents to the optical practice' Information Governance Lead to ensure that they don't reoccur a second or third time.

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 electronically 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 information security

There are many ways to ensure good information security. 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. Take care to ensure the secure disposal of personal information, for example shredding spare forms or placing them in a designated confidential waste bin for secure destruction rather than the normal waste bins.
- **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 at the end of each day.
- **Passwords:** Choose a good password of at least 6 characters long, with a mixture of letters, numbers and symbols. Keep passwords secret and safe. Make sure you change your password at regular intervals.
- **Avoid inappropriate disclosures of information:** Make sure you don't discuss sensitive information in appropriate venues, e.g. in public areas of the practice.

When checking personal information, ask the patient to confirm their details to you, rather than you reading their details out loud.

- **Ensure the premises are secure:** If you're the last to leave the practice at the end of the working day, make sure windows and doors are locked. If there is a burglar alarm make sure it's turned on.
- **Seek advice from you Information Governance Lead:** Make sure you know who is responsible for Information Governance in your optical practice and ensure that you seek his/her advice on information governance issues.
- **Follow optical Information Governance policies and procedures:** As part of the NHS Information Governance requirements, all optical practice 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 Information Governance lead on what procedures are in place for your practice.
- **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 Information Governance issues in your practice.
- **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 information to removable media such as CDs, DVDs, and memory sticks if you have been authorised to do so. Unauthorised access to the information should be prevented by the use of encryption.

UK law says personal information must be protected

Why not work with your Information Governance Lead to think about additional measures you could take to protect information in your optical practice.

Case Study 2

John Smith walks into an optical practice and asks whether his glasses are ready for collection. The optometrist has been very busy and the optical assistant hands over the glasses in John Smith's records. Two hours later, another John Smith comes to collect his glasses, and it becomes clear that the wrong glasses have been given to the original John Smith. Both patients are extremely angry and the practice is left in a difficult situation. The optical practice carries out an internal investigation to try and identify who gave out the spectacles.

Question: What could have been done to avoid this situation?

Check your answers on page 16.

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

It is important that when a patient 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 conducting a sight test).

Accurate, accessible and complete records will also protect the legal and other rights of the optical practice, 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.

Optical practices are required by the College of Optometrists Code of Ethics to make and keep accurate and complete patient records. In addition, the Department of Health has issued guidance to the NHS titled Records Management: NHS Code of Practice which provides a framework for the management of records, including how long records should be kept, how they should be stored and what should be done with records that are no longer required.

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 they book an appointment.
- 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.

Question: Which Principle do you think has been breached?

Principle 1: Personal data shall be processed fairly and lawfully.
Principle 3: Personal data shall be adequate, relevant and not excessive for its purposes.
Principle 4: Personal data shall be accurate and where necessary kept up to date.
Principle 7: Appropriate technical and organisational measures shall be taken against unauthorised of unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Check your answers on page 16.

Case Study Answers

Case Study 1:

Answer: The staff member had no justified purpose for carrying out ANY of these actions. This scenario leads to: the need to discipline staff, loss of reputation for the practice and a risk (to the practice and 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. Staff members also have a confidentiality clause as part of their employment. The General Optical Council may take action against the optometrist and the practice is a complaint is received.

Case Study 2:

Answer: This situation could have been 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:

Answer: The correct answer is “Principle 4: Personal data shall be accurate and where necessary kept up to date”. The information in Steven’s record wasn’t kept up to date. This meant that his sight test appointment was delayed. Due to the error at the optical practice, Steven had to wait longer for his appointment.

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

Declaration of Completion of Training

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

Staff Member's Name	Signature	Date

Knowing your Information Governance Lead

If you have concerns about Information Governance in your optical practice or questions about the processes in place in the practice to ensure confidentiality, talk to the person responsible for Information Governance issues, or in their absence, the optometrist.

The Optical practice IG Lead is…….