Information Governance Workbook

For use by Practice staff who do not use IT Facilities

Hyfforddiant Llywodraethu Gwybodaeth
Information Governance Training
IGDC • DHCW

Introduction

This workbook aims to help you recognise the principles of Information Governance and understand how they apply in your everyday work.

What is Information Governance?

Information Governance is a framework, which supports how organisations and individuals manage the way information is handled. It applies to sensitive and personal information of employees, patients and service users. It also applies to information related to the business of the organisation. It is about setting a high standard for the management of all information and giving organisations the tools to achieve that standard. Information Governance ensures that all of the information held by the organisation is used fairly and lawfully and handled appropriately.

Who does it apply to?

Information Governance applies to **ALL** employees, including but not limited to facilities staff, administration staff, nurses, doctors, consultants, pharmacists, dispensary staff, etc. It also applies to anyone coming onto the Practice site for any reason, for example window cleaners, repair/maintenance companies and their staff, agency staff, work experience, students, confidential waste companies, etc.

For example:

Facilities staff will have access to locked areas including swipe card accessed areas, information may be delivered by delivery services around the Practice Cluster, and all staff will be recorded at some point on CCTV systems.

If you have access to personal/patient/business information, then information governance applies to you.

For the purpose of this guide this information will be referred to as "confidential information".

Data Protection and Confidentiality

What is personal information?

Personal information is information which relates to an individual i.e. a patient or employee, who can be identified either directly or indirectly by the information.

Personal data may also include special categories of personal data which is considered more sensitive. Examples of special category data includes data concerning health, or data which reveals an individual's racial or ethnic origin or trade union membership.

All staff have a legal obligation to respect the privacy of patients and other employees, and to act appropriately when handling personal data.

Examples of personal data include:

- Personal information about any individual such as name, address, date of birth, etc;
- Pictures, photographs, videos, audiotapes or other images of a patient/individual;
  Medical information, such as NHS number, health, medication, treatment dates, sample types, screening information, etc;
- Staff information including personal files, occupational health files, complaints or financial information such as payroll, expenses, pension, etc.

Local Policies & Procedures

The Practice will have a number of policies and procedures in place to assist staff in complying with legislation and national standards. All staff should ensure that they are familiar with the Practice's policies and procedures, if you are unsure how to access these please ask your supervisor.

The Confidentiality: Code of Practice for Health and Social Care in Wales also provides guidance on how to keep information confidential. Copies of this should be made available to you.

Data Protection Legislation

Data protection legislation (including the UK General Data Protection Regulation 2016 (UK GDPR) and the Data Protection Act 2018 (DPA)) protects how a living person's information is used. It is a criminal offence to share information unlawfully under these regulations.

The Information Commissioners Office (ICO - https://ico.org.uk/) is the regulatory body that ensures compliance with the law and may impose penalties for non-compliance. Penalties include fines or prosecution and can apply to both individuals and organisations. Potential penalties can include fines of up to 4% of an organisation's annual global turnover, or £17.5 million (whichever is less), as well as criminal convictions and prison sentences.

Mail

Incoming mail marked 'confidential', 'F.A.O', 'private', 'addressee only' or similar must be passed to the person or department it is addressed to.

Outgoing mail (sent internally and externally) containing confidential information must be sealed securely (double enveloped if necessary), marked 'Private and Confidential' and fully addressed to a named individual, with their post title if known.

Bulky documents or records which contain confidential information, such as copies of medical records should be packaged securely (double enveloped if necessary) and sent via recorded delivery service as a minimum.

Note: original records should never be released unless subject to a court order

Faxing

Fax should **only be used as a last resort**, if there is any doubt **DO NOT** send confidential information by fax. Where no alternative is available the use of fax may be considered, providing the 'Safe Haven' principles are followed:

- The fax machine is located in a secure, restricted access area;
- Frequently used fax numbers are carefully programmed into the fax machine and tested to minimise the risk of misdialing (this includes both internal and external fax numbers);
- A fax cover sheet is used containing a confidentiality statement, the number of pages and contact details of the sender;
- The fax number is checked with the person you are sending it to;
- If you do not know the person you are sending it to, additional checks are carried out to make sure that the person is allowed to have this information;
- If you are faxing confidential information, you must seek confirmation that it has arrived safely

If you have a role where you access lots of different areas within the Practice and you see the fax machine is not in a secure area such as open reception areas where anyone can see the information (i.e. patients, relatives of patients, members of the public, etc.) please notify your Supervisor.

Verbal Communication

The Practice should have a procedure in place which gives guidance on disclosing confidential information, if you are unsure how to access this please ask your Supervisor. However, the following basic rules should be applied:

- Unless absolutely necessary, such as in a life-or-death situation, confidential information must not be disclosed verbally to anyone whose identity cannot be verified;
- If the information is about a third party, you must ensure the individual has appropriate authority to receive information about the other person;
- When speaking to anyone about a confidential issue, you must ensure that you cannot be overheard by anyone.

Storing & Transporting Confidential Information

The Practice should have a procedure in place which gives guidance on the safe storage and transportation of confidential information, if you are unsure how to access this please ask your Supervisor. However, the following basic rules should be applied:

- Confidential information **must not** be taken home;
- Documents transported in a vehicle must not be visible to anyone or left in a vehicle for long periods of time, particularly overnight;
- When transporting any documents, they must be carried securely, even when transporting between Practices, to ensure that they cannot be lost, dropped or exposed to weather conditions.

If part of your role is to deliver information around the Practice, you must ensure that this information is never left unattended.

Confidential Waste

The Practice will have a procedure in place that provides guidance on the handling of confidential waste, if you are unsure how to access this please ask your Supervisor. However, the following basic rules should be applied:

- All confidential paper waste must be shredded on site or collected and securely destroyed by an approved third-party contractor, confidential waste should not be transported between sites unless done so in line with the Practice's Safe Storage & Transport of Confidential Information procedure; Whilst awaiting collection or shredding, confidential waste must be stored safely and securely within confidential waste bins at all times. It is important that confidential waste is not confused with general waste;
- If shredding onsite, confidential waste should be shredded as soon as possible;
- Certain information has minimum retention periods, if you need to know how long information needs to be kept for then you can seek advice from your Supervisor;
- Every site should have proper arrangements in place for disposing of electrical/IT/computer items, as these items often contain confidential information, it is important that these types of items are not confused with general waste;
- Other items may also need to be destroyed under special conditions, such as fax carbon rolls, video tapes, slides, etc. Again, it is important that these items are not confused with general waste. If you need further information, you can seek advice from your Supervisor.

Information Security

The Practice should have a procedure in place which gives guidance on information security, if you are unsure how to access this please ask your Supervisor. However, the following basic rules should be applied:

- Staff should make sure that confidential information is not left unattended, particularly in areas which may be accessible by the public;
- If you see any computer screens containing confidential information which has been left unattended, please raise this with your Supervisor or a manager in that area;
- You should NOT read information that has been left unattended i.e. on computer screens, patient files left on desks, etc;
- Consider local security measures, particularly if based on ground floors or in busy, publicly accessible areas, for example, ensure blinds, windows, doors, etc. are closed and secure;
- If working in areas where doors have been locked by staff and access is required, i.e. to clean, empty bins, then each room must be opened, cleaned and locked one at a time. Rooms should never be left open and unattended;
- Staff should wear ID badges and visitors should be met and escorted wherever possible;
- Users should not attach any privately owned portable storage devices (including USB sticks, phones, cameras etc.) to any Practice equipment.

It is everyone's responsibility to maintain a high level of security. Remember this could be your or your family's information.

Phones / Photographs / Dictaphones / Social Media

The Practice should have a procedure in place which gives guidance on taking pictures, or recordings of patients, staff and visitors. If you are unsure how to access this, please ask your Supervisor. However, the following basic rules should be applied:

- Personal mobile phones should only be used on breaks in areas where it is allowed. If you are going to use social media i.e. Facebook, Twitter, Instagram, etc. please be aware how this may look to others;

- You must never post anything on social media about what you see or hear in work;

- Photos/recordings must not be taken of anyone without their consent;
  If you are aware/see someone taking photos/recordings and you do not think they have asked permission, then please notify your Supervisor or a manager in the area.

Records Management

The Practice will have a procedure in place that provides guidance on records management, if you are unsure how to access this please ask your Supervisor. However, the following basic rules should be applied:

- All records should be stored safely and securely and be accessible when needed;
- Removable storage should be encrypted i.e. USB sticks, CD's, DVD's, Dictaphones, tablets, laptops, etc;
- If you see any records which are not stored safely and securely, then please raise this with your Supervisor and/or a manager in that area as this will need to be reported as an incident.

Requests for Information

Patients and staff can make a request for information held about them by the practice under data protection legislation, this is usually referred to as a Subject Access Request (SAR). The practice should have a procedure in place for managing these requests, therefore seek assistance from your Supervisor. SAR requests can be made verbally and are not required to be made in writing. SARs have strict timescales under which they must be responded, therefore if you receive a request, you must inform your supervisor/manager **immediately**. You must **NOT** respond to a request yourself; the Practice will have a designated individual responsible for responding to these types of requests.

Anyone can make a request for non-personal information about the Practice under the Freedom of Information Act (FOIA) or the Environmental Information Regulations (EIR). For example, what cleaning products you use; what the average waiting time for an appointment is, etc. If the practice holds the requested information, they are legally required to share it using the correct procedures, unless a specific exemption applies. Requests under FOI and EIR have strict timescales under which they must be responded to, therefore it is vital to pass any requests you may receive to your supervisor/manager **immediately**. You must **NOT** respond to a request yourself; the Practice will have a designated individual responsible for responding to these types of requests.

Incident reporting

- It is extremely important that if you are worried about anything you see or hear, that you discuss it with your Supervisor as soon as possible and report it as an incident if appropriate;
- If you work in an area where you are providing a service i.e. domestic services, making deliveries, etc. and are given confidential information accidentally i.e. patient notes left lying in plain sight, or notice a
  USB memory stick in a bin etc. please raise this as an incident with your Supervisor as soon as possible;
- The Practice has a duty to report certain types of data breaches to the Information Commissioner's Office within 72 hours of becoming aware of a breach, therefore it is extremely important that any incidents or potential incidents are escalated to your supervisor and reported as soon as possible.

Where can I find assistance?

Any issues/concerns should be raised immediately with your Supervisor/Practice Manager.

Once you have completed this workbook, please go on to populate the IG assessment attached.

Information Governance Assessment for Practice Staff

Once you have read the Information Governance Workbook, please complete this assessment.

Full name:

Staff number:

Practice name:

Date completed:

Final Score:

1. Who is responsible in the Practice for the security of confidential information? (**select one option**)

- All staff with access to computers
- Only clinical staff
- Only staff employed in security management
- Everyone
- Only line managers

2. When no longer needed, which of the following should be confidentially deleted or destroyed, and not discarded as normal rubbish? (**select two options**)

- DVD containing a training presentation
- Diabetic patient information leaflet
- List of patients being referred to antenatal classes
- Published minutes of a Management meeting
- Old computing equipment

3. What are the possible consequences of failing to protect confidential personal / patient information? (**select four options**)

- A loss of trust by patients/staff/public
- Distressing social media posts
- Recognition award for hard work
- Compliment from a patient
- Patients targeted by dishonest retailers
- Financial penalty or imprisonment for an individual

4. You notice a USB stick in a bin at the reception desk. What should you do? (**select one option**)

- Leave it where it is, it is not your responsibility
- Take it home to see what is on it
- Place it back on the desk, it must have fallen in accidentally
- Hand it in to the Practice Manager and report it as an incident

5. You find a bundle of papers on a chair in a public waiting room. They are patient questionnaire responses, what should you do? (**select one option**)

- Put them in a waste bin to tidy the place up
- Put them in a confidential waste bag
- Pick them up and put them on a nearby desk
- Hand them to a manager and report the incident
- Staple them together and use them as notepads to save paper

6. You have walked through the reception area and see your neighbour's name appear on the appointment announcing display screen. What should you do? (**select one option**)

- Phone your neighbour's partner to let them know that your neighbour is at the practice
- Look for them and pop over as you're sure they would want to see you
- Post on Facebook that you saw your neighbour in your workplace
- Carry on with your work

7. You are stopped in the corridor by a member of the public wanting a copy of their test results from last week. Is this a valid subject access request (SAR)? (**select one option**)

- Yes
- No

8. You are on Facebook on your mobile at home and see a post from a friend who also works in the same practice pharmacy, asking if anyone knows where the key is kept for the cupboard containing prescriptions for collection. What do you do? (**select one option**)

- Nothing as you don't know where the key is kept
- Respond to say that you'll ask around tomorrow in work
- Respond to say that it's probably with all the other keys in the top drawer of the unlocked filing cabinet in the office
- Do not respond and report it to your supervisor as soon as possible

9. As part of your role, you have been given access keys / swipe cards to restricted areas / locked offices etc. What do you do? (**select one option**)

- Unlock all rooms / offices in a particular area first before performing your duty as it will be quicker this way
- Unlock each room / office as you're going along and lock it again as soon as you've finished in it to ensure that the area remains as secure as possible
- You've forgotten your access card, so borrow one from a colleague making sure you lock each room when you've finished in there.

10. If you come across a colleague disposing of their old computer within the general waste, what do you do? **(select one option)**

- Ignore it and carry on with your day
- Stop and offer them a hand with the disposing of the computer
- Stop and inform them that there should be proper arrangements in place for disposing of electrical/IT/Computer items

Please return this form to your manager, if you do not achieve **80%** you will be asked to complete further training.

Final Score: ___ / 14 Percentage: _____%