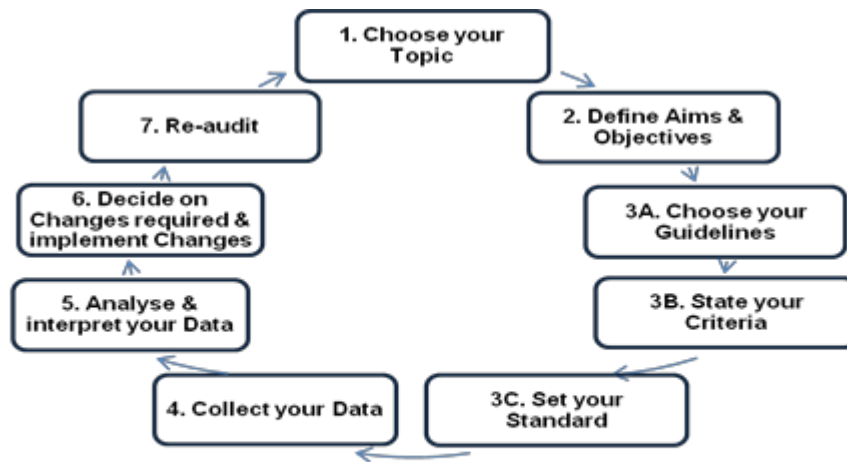




Audit of Data Protection and Information Management



AUTHOR

Mary Fanning, Clinical Audit Facilitator Substance Misuse Programme ICGP

Purpose of ICGP sample audits

The purpose of the ICGP sample audits is to provide practitioners with suggested audit topic proposals and related tools in order to aid them in carrying out an audit in this topic area. For each topic, a specific guideline is chosen which identifies best practice for the relevant topic. Following this, examples of the elements of compliance that could be measured are provided - referred to as "criteria". Finally, examples of the type of data that is required in order to audit the sample criteria are provided. The overall ICGP audit toolkit provides detailed generic instructions on how to carry out and report your audit.

Disclaimer

In all instances where 'your patients' are referred to, this can be taken to mean the patients you see. Where 'your practice' is mentioned, this refers to the work you do, not necessarily that you need to be based in one particular practice."

Audit Topic

Data Protection and Information Management.

Aims and Objectives

To ensure that the information obtained by staff members of the practice is managed in accordance with Data Protection legislation.

This audit could be included under the domain of 'Management', in particular for the practice data controller.

Evidence/Guidelines

'ICGP Guide to the Data Protection Legislation for Irish General Practice April 2011'.

Sample Criteria

1. The practice is registered with the Data commissioner and has appropriate measures in place to protect patient information

Questions 1, 2, 5, 8, 9, 10, 11, 13, 16 and 17 on the data collection form below are appropriate to measure your practice against this criterion.

2. The practice has taken appropriate measures to ensure that patients are aware of who has access to their information

Questions 6 and 20 on the data collection form below are appropriate to measure your practice against this criterion.

3. There are policies and procedures available in the practice that guide staff on how to protect patient information

Questions 3, 4, 7, 12, 14, 15, 18 and 19 on the data collection form below are appropriate to measure your practice against this criterion.

Choose the criteria (criterion) from the above on which to conduct your audit and then set your standard (sometimes known as your target). This is your desired level

of performance and is usually stated as a percentage. Beware of setting standards of 100%; standards should be realistic (perfection may not be possible).

Collect the Data

Using the form provided below, record yes or no for each question. Answering yes denotes compliance.

Decide on changes required and implement necessary changes

Analyse the data by checking the number of Yes answers and comparing to the targets set i.e. to the standard expected.

Put in place any changes necessary to meet the standard. Make a plan and assess what is required to bring the standard to a higher level. Involve all relevant staff of the practice to assist in meeting the standard.

Re-Audit

Use the same data collection tool and re-audit within a realistic timeframe. Compare results to see if there is an improvement since first audit.

References:

'ICGP Short Guide to Audit' (May 2011) Prepared by Claire Collins – Director of Research ICGP' Available on www.icgp.ie/audit
ICGP Guide to the Data Protection Legislation for Irish General Practice April 2011'. Available on www.icgp.ie

Data Collection Form for Audit of General Practice Data Protection and Information Management		Yes	No
Q1	The Practice is registered with the Data Protection Commissioner		
Q2	There is an identified person responsible for Data Protection in the practice (check)		
Q3	There is an information management policy for the practice		
Q4	Staff of the practice have been trained in confidentiality and privacy (ask all members of practice staff or check Training Records)		
Q5	There is a confidentiality agreement with hardware and Software support companies (ask to see)		
Q6	Information leaflet on data protection has been given to all patients (randomly check 5-10 records)		
Q7	There is an agreed data collection form for all new patients (randomly check 5-10 recent records)		
Q8	Password required to access all PCs and servers (check all)		
Q9	All users have own user name and password (Ask all staff)		
Q10	Permissions set to allow only authorised staff to access data (check)		
Q11	Computer monitors and paper records are secure (assess risk of unauthorised access)		
Q12	There is a policy on information sharing that staff are aware of (Ask all staff members and check policy document)		
Q13	Laptops and mobile devices are encrypted		
Q14	GPs and practice manager are aware of data retention periods (check)		
Q15	There is a practice policy on use of the internet (check policies)		
Q16	Staff members are aware that patient information cannot be sent by email (ask)		
Q17	Records are backed up daily (check)		
Q18	Staff members are aware of procedure for amending records (ask all staff)		
Q19	Staff members are aware of procedure for sending confidential information by fax (ask all staff)		
Q20	There is a notice in the waiting area informing patients of who has access to their information		