Clinical records management policy

Introduction

Effective storing and management information is important to ensure the smooth working of the Practice and to enable it to meets its statutory responsibilities. To achieve this information needs to be readily identifiable and accessible to all those who have a legitimate need to see it.

The Freedom of Information Act 2000 requires all public organisations to implement a code of Practice for Records Management based on the mandatory Code of Practice developed by the Lord Chancellor's Office under Section 46 of the Act.

Aim

To set out the process for storing and managing information, in order to ensure records are appropriately managed and easily accessible.

Background

There is a direct and indirect regulatory framework governing Records Management:

- Direct:
  - Freedom of Information Act 2018
  - Section 46 of the Freedom of Information Act 2000
  - The Lord Chancellor's Code of Practice
  - Code of Openness in the NHS (1995)
  - Public Records Act (1958)
  - Welsh Health Circular (WHC) (99)7 – Preservation, Retention and Destruction of GP General Medical Services Records relating to Patients.
  - Welsh Health Circular (WHC) (2000) 71 – For the Record

- Indirect – good practice under:
  - The Caldicott Report 1997
  - The Data Protection Act 1998
  - The Human Rights Act
  - The Medical Records Act Principles
  - The NHS Baseline IT Security Standards
  - Department of Health, Records Management: Code of Practice (2006)

Records should be managed in line with ISO standard 15489-1:2016. This sets out characteristics of effective records management. Records should be:

- Authentic – they are what they purport to be.
- Reliable – full, accurate, contemporaneous
- Integrity - complete, unaltered, protected against edit where appropriate, have an audit trail of any alterations.
- Usable – located, retrievable, presented, interpretable.

Records must be stored in a way that is easily identifiable and recoverable though out the documents lifecycle. There must also be a clear record of who has access to the records.

Action

Records containing personal or patient identifiable information will be managed in accordance with the principles of the Data Protection Act. The Practice has a file structure for filing both patient and non patient information. Paper patient records are filed alphabetically and stored in an appropriate way. Paper Non patient and business information is stored in either the Practice Manager's office or in the Practice archive.

Patient electronic records are stored in the Practice clinical system and must be kept tidy. This involves effective read coding for ease of searching and ensuring that sections such as the problem lists are kept to a minimum. This is done by checking the list or consultation notes before entering a first instance of a problem.

Non patient electronic records are stored either on the Practice shared drive, or for sensitive business / personnel records on the hard drive of the Practice Managers computer. The latter is regularly backed up onto a flash drive.

Staff responsibilities

Records Management will be the responsibility of the Lead GP, delegated to the Practice Manager.

Any staff member creating a new patient record is responsible for ensuring that it is created inline with the Practice policy. In addition, they are also responsible for ensuring that the contents of the records is accurate and that the record is stored correctly so that it can be easily retrieved.

Creation and use of patient records

All patient records must contain accurate information reflecting what was said in the consultation. The consultations are generally problem based, in that generally a problem should be entered at the start of the consultation. This allows for consultations to be easily found, see the progression of a condition or see how many times a patient has attend for the same or similar conditions.

Consultation and referrals must be written in clear language that another reasonable medical professional can understand.

A patient's records must only be used for the provision of medical and social care for that patient or providing information as authorised by the patient or their approved representatives.

All information relevant to the patient should be filed in their medical records and should not be filed elsewhere. All electronic records should be searchable by individual personal identifiable information. All paper records should be filed alphabetically by surname then 1st name.

Data for patient records is collected though consultations, information provided by outside agencies and relevant third parties such as patients relatives and carers. It is used for the purposes of providing medical care to patients.

This will be backed up by Practice privacy notices covering how and what information is collected, how it is used, shared, stored and disposed of. The notice will also cover how the practice ensures that only the minimum necessary data is collected and retained.

Maintenance of patient records

It is good practice to review patient records. Patient records generally should be reviewed and audited periodically to check the patient is still registered. This can be done by running a search on the clinical system to check when the patient last had some contact with the surgery. If the last contact was more than 7 years ago, a letter can be sent to the patient to check if they are still living at their registered address. If no response is received, steps should be taken to deregister the patient. The patient records (electronic and paper), so be periodically audited against the list of recent deregistration's and deaths, to check all files have been returned appropriately.

Patient's individual electronic records should occasionally be reviewed by a clinician to ensure all the information is relevant and easy to use. The most common issue is problem lists, especially for those patients transferring in from other surgeries. It is not necessary to record every minor issues a current, significant problem. Therefore, minor conditions can be moved into the past problem list and other issues can be combine or evolved as appropriate. Particular attention should be given to type of problem (is it recorded as new, review, end etc) to ensure there aren't two new problems recorded for the same condition for instance.

Retention and Destruction of Records

The Practice has a document retention schedule that has been drawn up in line with current NHS Guidelines (Department of Health (Whitehall) guidance, WHC (2000) 71 and HSC/217 1999 and WHC (99) 7.

Physical and electronic records must be stored securely at all times. The PM will carry out a security risk assessment and audit at regular intervals and after any change to access and security arrangements. These risk assessment and audits should be reviewed by the Partnership and any remedial actions necessary, taken within a reasonable time frame.

Patients who de-registered should have their records passed onto the surgery the subsequently register with. If no such registration takes place, the records should be sent back to Shared Services within a reasonable time period.

When a patient dies, their records should be processed within a reasonable time period and then sent back to Shared Services. These records will be retained in accordance with NHS Wales rule (generally for 10 years after the date of death) and then destroyed.

Monitoring and review

The PM has operational responsibility for ensuring that the processes outlined above are adhered to and updated following any changes in procedure.

Outcome

- Understanding of the process for information storage and management

Conclusion

Effective storage and management of paper and electronic records is important to ensure that information is easy to locate and access. Record location lists need to be kept up to date also. In addition to ensuring information is easily accessible, regular management of information stores helps to ensure they do not become cluttered with information that is no longer relevant.