FACTSHEET

MEDISEC

We look after you

Storage and Retention of Medical Records

The Medisec team frequently receives queries regarding storage and retention of medical records, particularly from members who are moving premises or upgrading systems. This is a short overview of your ethical obligations and the appropriate retention periods for different categories of records.

Storage of Medical Records

The Medical Council *Guide to Professional Conduct and Ethics for Registered Medical Practitioners* (available on the Medical Council website) states doctors must comply with their obligations under Data Protection legislation in relation to secure storage and eventual disposal of patient records.

All confidential records including handwritten notes, computer generated records, test results, copies of correspondence etc should be stored securely and protected against accidental loss, including corruption, damage or destruction at all times.

It is best practice to avoid carrying clinical records in a car, for example, when doing home visits. Any laptop or remote devices with access to patient records should be fully secure and encrypted.

All practice administrative staff should be aware of their confidentiality obligations, for example locking paper records away in a suitable filing cabinet and ensuring security of computer systems. Technology is not foolproof and regular back-up should be ensured.

Retention of Medical Records

In compliance with the Data Protection Acts, "Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed".

The retention periods for medical records are taken from the HSE 'Record retention periods (2013)[2] and also detailed in ICGP *Processing of Patient Personal Data: A Guideline for General Practitioners v2.3*[3]. These periods are also in line with the recommendations of Medical Indemnity Agencies and the Health Information and Quality Authority (HIQA).

Please see the table below.

Type of Patient Record	Retention Period
Adult/General	8 years after last contact.
Deceased patients	8 years after date of death.
Children and young people	Retain until the patient's 25th birthday or 26th if young person was 17 at the conclusion of treatment, or eight years after death. If the illness or death had potential relevance to adult conditions or genetic implications, specific advice should be sought as to whether to retain the records for a longer period.
Maternity (all obstetric and midwifery records, including those of episodes of maternity care that end in stillbirth or where the child later dies)	25 years after the birth of the last child.

Mentally disordered persons (within the meaning of the Mental Health Acts 1945 to 2001)	20 years after the date of last contact between the patient and the doctor, or eight years after the death of the patient if sooner.
Patients included in clinical trials	20 years.
Suicide - notes of patients having died by suicide	10 years.
Cause of Death Certificate Counterfoils	2 years.
Records/documents related to any litigation	National Hospital Office recommends that the records are reviewed 10 years after the file is closed. Note however, if the litigation related to a child, this should not be used to lessen the retention period set out above.

The ICGP advises in its document: *Processing of Patient Personal Data: A Guideline for General Practitioners v2.3 (2019),* available on the ICGP website- "*At all times the interest of the patient must be to the forefront. If it is not in the interest of the data subject, then the medical records should not be deleted. For example, a 25-year-old man has treatment for a malignant melanoma and after recovery is not seen in the practice for 8 years. It would not be in the interest of the patient to delete his medical records. On the other hand, it would not be appropriate to retain data on an 87 year old woman who died 8 years ago, following a stroke, and had no history of a major mental health disorder.*"

It is appropriate to securely dispose of obsolete medical records but doctors should decide carefully what records should be retained and what records may safely be destroyed.

Records belonging to current patients must be kept. If storage arrangements for paper files might pose a risk to the security or integrity of the records, they should be scanned carefully and saved electronically so that the hard copies can be securely destroyed.

Register of records destroyed after retention period

Healthcare records which have reached their official retention period, should be reviewed under the criteria issued by the HSE to check if they should be destroyed. If records are to be disposed of, it is vital to do this in a way which maintains the confidentiality of the records. According to the HSE guidance, a register of records destroyed should be maintained as proof that the record no longer exists.

The register should show:

- name of the file
- former location of file
- date of destruction
- who gave the authority to destroy the records

For healthcare records, the register of records destroyed should also include:

- healthcare record number
- surname
- first name
- address
- date of birth

May 2020

Adhering to the above best practice should assist in preventing or defending any complaints relating to the storage and retention of patient records. If you have any queries in relation to the above, please do not hesitate to contact a member of the Medisec advisory team.

May 2020