Risk Control

Medical and Health Records: Risk Issues and Management

The paper or electronic patient health record serves two major purposes: communicating information both within and outside the practice/clinic setting about a patient; and creating a written history of patient care in the event of later questions or challenges. The record serves as objective documentation of all phases of treatment, including diagnosis and assessment, laboratory testing, and treatments used and the patient's consent for them.

Every provider setting needs a written policy governing professional documentation and record management. The policy should address, among other issues, patient confidentiality, privacy, and the release and retention of records. Auditing adherence to the policies in place is as an important part of governance required for good records management, so ensure regular records audits are part of the annual audit plan.

The following strategies can help minimize liability exposures related to documentation and record management.

1. General Documentation Guidelines

Sound documentation is fundamental to risk management. The following general principles of documentation can help the practice maintain consistent, professional patient healthcare:

- Ensure that any paper notes are legible, written and signed in ink, and that all records include the date and time of entry.
- Avoid subjective comments about the patient or other healthcare providers.
- Do not erase or obliterate notes in paper records in any way. This may suggest an attempt to purposefully conceal an error in patient care. Draw a line through it.
- Document actions and patient discussions as soon as possible after the event to ensure accuracy of the entry.
- Include all vital information such as date of dictation and transcription when dictating notes (as applicable).
- Never alter a record or write a late entry after a claim has been filed.
- Develop a list of approved abbreviations for use in documentation.

2. Hybrid Records

During the transition from paper to electronic health records (EHR), "hybrid" records – part paper, part digital – may be used during the transitional period. To simplify the transition, consider the following risk management interventions:

- Determine the components of the patient healthcare record that will remain in paper form during the transition and devise policies to protect and preserve data maintained in a hybrid state.
- Identify areas of potential duplication across paper and electronic systems, and reduce or eliminate potentially confusing redundancies.
- Risk assess to ensure that all aspects of clinical care can continue if one department moves to EHRs and others do not, e.g., if a patient needs to transfer between departments ensure all care can be handed over.
- Establish written parameters for use of paper notes in the hybrid record in order to reduce the risk of missing or inconsistent electronic documentation.
- Ensure that clinic staff possess the necessary IT competencies before proceeding with EHR implementation.

- Acknowledge the increased workload implications of a newly implemented EHR, and provide appropriate support in the form of additional hands-on training, etc.

3. Record Retention

A practice/clinic must maintain the patient health records in accordance with: professional standards of practice; and at least the period of the applicable statute of limitations for malpractice. For minors, health information should be archived until the patient reaches majority plus the period of the statute of limitations. It is prudent to err on the side of longer retention, as the statute may not be triggered until the potential plaintiff learns of a possible connection between an injury and care received.

Although there is no single record retention schedule that every healthcare professional must follow, healthcare leaders should be aware of rules and recommendations from professional associations, among others.

By implementing legally compliant record retention and maintenance policies, an organization can help ensure that vital documents are accessible for clinical and legal purposes.

4. Record Release

As a general rule, information about a patient should be disclosed only on the written authorization of the patient or the patient's substitute decision maker. The patient has right of access to the information in his/her personal health record and to a copy of the record. Third parties, including spouses, parents of adult children, children of aged parents, and siblings require written patient authorization to obtain a copy of the record. Lawyers representing patients are required to have written patient authorization to obtain a copy of the record.

Patient consent for disclosure of personal health information is not required for referrals to or consultations with other healthcare providers. The record may also be released without patient consent on receipt of a court order, or when the request is expressly for a purpose authorized by legislation.

When a patient record is requested, and written patient authorization is obtained:

- Release only a copy of the health record – never the original.
- Respond to patients' requests for a copy of their own health records in a reasonable time and manner.
- Charge the patient the amount of reasonable cost recovery for a copy of his/her own health record unless this fee is prescribed.
- Document the request and date the copy was sent or picked up in the patient healthcare record.
- File all original patient authorizations for release in his/her record.
- Ensure third party references are appropriately redacted prior to release, in order to protect others' confidentiality.

5. Patient Health Record Retention and Storage

Retention periods for patient health records can vary significantly from jurisdiction to jurisdiction. A record should be retained from date of last entry in the record for the period set by professional standards of practice (or policy) and the jurisdiction's statute of limitations for malpractice. The record of a minor has to be retained until the minor reaches the age of majority plus the limitation period.

Decisions regarding suitable record storage are influenced by: access requirements; security concerns; cost; and business continuity.

Paper records that are accessed on a daily, weekly or monthly basis should be stored on-site for ease of access. All recordkeeping systems, whether paper or electronic, must provide controls to ensure that only authorized users have access to the records. For physical media such as paper, records should be stored where there is controlled access such as a locked cabinet or room, and not open shelving accessible to unauthorized individuals (e.g., patients in a waiting room).

As it is not uncommon for computer systems to fail, strategies against the loss of patient information contained in an EHR should be considered. In some jurisdictions, legislation and regulatory authority policies require that electronic files are routinely backed-up and that the system allows files to be recovered. Even if there are no specific regulatory requirements in a particular jurisdiction, it is a good practice to back up patient information daily or weekly and to ensure the backup files are encrypted.

When storing inactive records, records storage, either on- or off-site, should be physically secure and environmentally controlled to protect records from unauthorized access and damage or loss due to temperature fluctuations, fire, water damage, pests and other hazards. Any suggested storage location (e.g., basement) should be assessed for suitability against these considerations.

Backup copies of records (paper or electronic) may be retained off-site in a protected environment to resume business after a disaster or to retrieve a replacement copy of a lost or damaged record. The backup system is vital in case an office computer, laptop or other digital device is stolen, lost, or destroyed records.

Ensure that business continuity plans require tests of the organization's ability to retrieve the record in its complete form in a timely manner.

For additional information visit cnacanada.ca.