Guidelines for Electronic Medical Records and Role-Based Access

This section will:

- Summarize privacy and security considerations during the transition from paper to EMR.
- Define role-based access and identify key considerations related to EMR implementation.
- Identify privacy and security best practices.

Making the Transition to EMR

The provider-centric model of data stewardship is one where a physician practising in a clinic environment maintains a medical record of care provided to an individual patient. That medical record can be in paper or electronic form but the principles of physicians' data stewardship remain the same.

The transition from a traditional paper-based patient record to an electronic system that uses new technologies is a significant undertaking, requiring changes to a practice from many perspectives – clinically, administratively, and organizationally. Physicians must be prepared to maintain the protection of personal health information during the transition period where both paper and electronic versions exist in parallel.

During the transition to EMR, the following recommended steps may be of assistance:

- Understand existing paper-based workflow processes including data flows and modify processes as necessary to integrate the use of EMR to achieve the greatest benefits.
- Assess existing privacy and security policies and practices and revise them to reflect the use of EMR and personal information in electronic format.
- Update staff privacy training to incorporate an understanding of the changes associated with EMR.
- Begin by scanning paper records into electronic format or start entering data into the EMR beginning on day one.
- Retain one original medical record and once the information has been fully transitioned to EMR, the original paper record may be securely disposed of.
- If only part of the paper record is transitioned to EMR, retain the remainder of the paper record as part of the original medical record.
- Save scanned copies of paper records in "read-only" format.
- If using optical character recognition (OCR) technology to convert records into searchable and editable files, retain either the original record or a scanned copy.

- Ensure patients still have access to their complete information upon request, even if the information now exists in a combination of formats (paper, electronic, digital).

Role-Based Access

Role-based access control is an essential functionality in an EMR system. Role-based access uses information technology to protect the personal information of the patient by ensuring that access to the patient's personal information is based on the "need to know" and **"**least privilege**"** principles.

The role-based access model identifies all possible roles that require access to a patient's personal information, and assigns each of these roles access to only the type and amount of personal health information needed to perform the job function. For example, specific permissions (e.g., reading, writing, printing) can be assigned to certain personal health information (e.g., lab results, medication information, registration information) based on the job duties of the person who has access.

Roles must be defined for all of the various users, whether they are employees or otherwise, who access the EMR. These include clerical staff, billing services, nurses, students, residents, physicians-in-training, locum physicians, on-call group, visiting specialists, and other physicians within the practice. When assigning a role, a prudent physician will always assess the degree to which access to the patient's personal information is truly necessary for that person to perform their duties.

Implementing this model also allows for ease of account management when setting up new users and modifying accounts. Role-based access models must be designed to support both business and clinical workflow, and as such the EMR software must have flexibility to support the unique needs of each practice. It must also allow for exceptions to the standard role and permissions, provided it is authorized and necessary for the performance of job duties.

An authorized role alone does not entitle an individual to access a given record, as the individual must have a "need to know" based on that individual's provision of care to the patient. "Need to know" can frequently become "want to know", which may not meet the required threshold for granting authorized access or may lead to workplace snooping.

When determining which functional areas and permissions should be assigned to each role and user, ask:

- Can existing users currently access all of this information?
- Does each of these roles truly need access to all areas of available information?

- Are the users unable to carry out the requirements of their job if they do not have access to this information?
- Can the patient suffer harm if the user does not have access to this information?
- Are there professional practice standards requiring the user to have access to this information?
- Is the information required to support the care of the patient across the continuum of care?
- Does the user require regular and routine access to this information or does he or she only require access on an occasional basis where other methods of access may suffice?

When defining roles, assigning access and granting permissions associated with each role, ask:

- What are all the possible roles that would require access to personal health information in the practice?
- What are the possible functional areas when that information may need to be accessed (e.g., clerical, clinical, financial/billing)?
- What are all the possible permissions that could be assigned to each role (e.g., create, read only, update, delete)?
- Are there additional permissions that a user in a role could be assigned (e.g., mask/unmask information, print, email)?

Privacy and Security Considerations

Physicians are responsible for data stewardship, and assume responsibility for any access to personal health information, including by staff, contractors and delegates.

To be effective as a privacy-enhancing mechanism, role-based access should be used in conjunction with additional privacy and security controls, such as:

- automatic log off feature
- strong, up-to-date, industry-standard encryption applied to EMR data and portable electronic devices
- audit trails to record user access
- allowance for correction/annotation of information
- ability to mask/unmask sensitive data (See Guidelines for Consent and Masking Options)
- unique user IDs and passwords
- not granting access until the user is authorized by a physician, has completed training, is provided with privacy education, has signed a confidentiality agreement and is made aware of practice privacy and confidentiality policies

- ensuring that audit log capability is activated in the EMR system to track all user access to patient information for the purposes of compliance monitoring and incident investigation
- managing user accounts including adding, modifying, and de-activating user accounts on a regular and timely basis
- confidentiality disclaimers on printed reports
- robust backup and recovery procedures