**Policy Title:** Electronic Medical Records Policy and Procedure  

<table>
<thead>
<tr>
<th>Program Area:</th>
<th>All Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Identifier: (optional)</td>
<td>Effective Date: 11/14/2014</td>
</tr>
<tr>
<td>Approval Date:</td>
<td>Revision Date(s):</td>
</tr>
<tr>
<td>Approved by:</td>
<td></td>
</tr>
</tbody>
</table>
Kim Smith RN, BSN, MSHCA, Health Director  
Hilda Memory RN, BS, MSHA, Director of Nursing  
Mitzi Ward PA III  
Becky McDowell Patient Relation Representative IV |

**Purpose:**  
To ensure accurate and complete documentation of services rendered to CCHD patients, and to provide guidance to staff regarding EHR documentation.

**Definitions:**  
The Columbus County Health Department (CCHD) will strive for complete and accurate documentation in Electronic Health Records (EHRs) and will follow specific guidelines to ensure accurate documentation.

**Definitions:**  
1. **Patient:** For the purpose of this policy statement, “patient” includes anyone who: makes an appointment to receive services, applies for services of a specific program, or receives services from a Health Department staff member or contracting agency of the Health Department.

2. **Electronic Health Record (EHR):** The patient’s record that is maintained in the Columbus County Health Department’s CureMD electronic medical records system. The EHR includes a patient’s contact information, billing information, clinical documentation of services provided by CCHD, diagnostic test results, medical history, allergies, and may include health information from other providers.

3. **Provider:** Anyone employed or contracted by CCHD who offers medical or other clinical services to the patient.

**Management Support Staff:** Staff, who registers patients, enters or updates demographic information about the patient, provide appointments, and generate patient account statements.
## Responsibilities:

All CCHD clinical, laboratory, and management support staff and providers.

## Procedures:

### Establishing a Patient Medical Record:

When a patient calls or presents for clinical services at CCHD, Management Support staff will search for an existing EHR. If no record exists, an EHR will be established.

### Documentation Guidelines:

1. All entries must be factual, accurate, relevant, timely, and complete.
2. Refer to the CureMD Work Flow by logging on to CureMD and accessing the “Help” tab at the top of the page. Then, click on “Wiki” and enter your category into the search engine.
3. Clinical encounters will be formatted according to the established “Rules for Note Formats/Programs/Encounter Types” stored in the Clinical Policies and Procedures folder on the Health Department’s I-drive.
4. Signatures/initials entered into patient EHRs will be recorded in accordance with the CCHD legal signature list.
5. Unused sections (entire sections of a clinical encounter note that are not required for a particular patient visit/service) will be closed so that they won’t appear in a printed summary of the visit.
6. Only abbreviations and symbols recognized and approved by CCHD may be used in the EHR. Refer to the Abbreviations in Medical Records Policy for a list of approved abbreviations and symbols. Any additions or changes should be referred to the CCHD Nursing Director.
7. Errors discovered before notes are signed and locked may be corrected by the clinical staff who recorded the information. Staff should carefully review the information in the EHR as they enter it to ensure accuracy.
8. After a note is signed and locked, errors should be corrected by entering an “Addendum Note”.
   a. The Addendum Note must be affiliated with the original note in which the error resides.
   b. The Addendum Note should identify the error and should state the correct information.
   c. The Addendum Note must not be backdated, but should be dated on the day the Addendum Note was created.
9. Notes must be reviewed and signed promptly by appropriate providers.

## Maintenance and Security:
1. All management support and clinical staff, including contract providers, are responsible for the security of EHRs.
2. The EHR software application should only be accessed from CCHD computers with appropriate antivirus software.
3. It is the responsibility of each staff person and provider to set and secure their own EHR password.
   a. Passwords must be changed every 90 days.
      • Log on to the EHR. Select “Practice Administration,” select “My Profile,” and click the “Change Password” link. Enter the old password and the new password where indicated.
      • If a staff member or provider forgets their password, the individual must contact one of the Super Users (PA III, Account Tech. IV, Patient Relations Representative IV, Director of Nursing, or the Health Director). The Practice Administrator will create a temporary password for the user. That password will be given only to the staff member or provider, and the staff member or provider will be instructed to change their password when they log in.
   b. Passwords are never to be shared with others.
   c. Staff members are prohibited from allowing any other individual to enter information into a patient’s EHR under the staff member’s username and password.
4. Computer screens will be locked when staff or providers step away from their computer to prevent unauthorized access. Employees of CCHD will be made aware that access is allowed only to those EHRs pertinent to their official function or type of service they deliver. Intrusion into an EHR for curiosity purposes will not be tolerated and appropriate disciplinary action will result. Information from an EHR may not be shared with staff or others not involved directly in the care of that patient. When an employee accesses an EHR, that employee assumes the responsibility for the privacy and security of the information.
5. When staff or providers are no longer affiliated with CCHD, a Practice Administrator will inactivate the user from the system. Practice Administrators are also responsible for adding new users.

Laws and Rules:

1. ARRA – American Recovery and Reinvestment Act
2. HIPAA – Health Insurance Portability Accountability Act
3. Security of Health Data (GS 130A-374)
4. Confidentiality of Records (GS 130A-143)
Reference(s):

<table>
<thead>
<tr>
<th>Reference Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. HIPAA Policy</td>
</tr>
<tr>
<td>2. CCHD Computer Password and Security Policy</td>
</tr>
<tr>
<td>3. CCHD Confidentiality Policy</td>
</tr>
<tr>
<td>4. CCHD Privacy and Dignity of Patient Maintained Policy</td>
</tr>
<tr>
<td>5. CCHD Medical Records Policy</td>
</tr>
</tbody>
</table>