TEXTING
### MEDICAL RECORDS – REVISED STANDARD

<table>
<thead>
<tr>
<th>STANDARD / ELEMENT</th>
<th>EXPLANATION</th>
<th>SCORING PROCEDURE</th>
<th>SCORE</th>
</tr>
</thead>
</table>
| 10.00.00 Condition of Participation: Medical Record Services. | **The hospital must have a medical record service that has administrative responsibility for medical records.**  
A medical record must be maintained for every individual evaluated or treated in the hospital.  
The texting of patient orders is prohibited regardless of the platform utilized.  
In order to be compliant with the CoPs, all providers must utilize and maintain systems/platforms that are secure, encrypted, and minimize the risks to patient privacy and confidentiality as per HIPAA regulations and the hospital and CAH CoPs.  
It is expected that providers will implement procedures/processes that routinely assess the security and integrity of the texting systems/platforms that are being utilized, in order to avoid negative outcomes that could compromise the care of patients.  
§482.24 | **DOCUMENT REVIEW AND INTERVIEW**  
1. Review the organizational structure and policy statements.  
2. Interview the person responsible for the medical record (health information) service to determine that it is structured appropriately to meet the needs of the facility and the patients.  
3. **Verify the facility does not permit the texting of orders by physicians or other health care providers.**  
**CHART REVIEW**  
Review a sample of active and closed medical records for completeness and accuracy in accordance with Federal and State laws and regulations and hospital policy.  
- The sample should be 10 percent of the average daily census and be no less than 30 records.  
- Additionally, select a sample of outpatient records in order to determine compliance in outpatient departments, services, and locations. | □ 1 = Compliant  
□ 2 = Not Compliant  

This standard is not met as evidenced by:
### MEDICAL RECORDS – REVISED STANDARD

<table>
<thead>
<tr>
<th>STANDARD / ELEMENT</th>
<th>EXPLANATION</th>
<th>SCORING PROCEDURE</th>
<th>SCORE</th>
</tr>
</thead>
</table>
| 10.00.06 Security of Medical Information | **RELEASE OF INFORMATION or COPIES OF RECORDS**

The hospital must have a procedure to ensure the confidentiality of each patient’s medical record, whether it is in paper or electronic format, or a combination of the two, from unauthorized disclosure. Confidentiality applies wherever the record or portions thereof are stored, including but not limited to central records, patient care locations, radiology, laboratories, record storage areas, etc.

A hospital is permitted to disclose medical record information, without a patient’s authorization, in order to provide patient care and perform related administrative functions, such as payment and other hospital operations.

1. Payment operations include hospital activities to obtain payment or be reimbursed for the provision of health care to an individual.

2. Health care operations are administrative, financial, legal, and quality improvement activities of a hospital that are necessary to conduct business and to support the core functions of treatment and payment. These activities include, but are not limited to:
   - Quality assessment and improvement activities,
   - Case management and care coordination;

3. Ask the hospital to demonstrate what precautions are taken to prevent physical or electronic altering of content previously entered into a patient record, or to prevent unauthorized disposal of patient records.

4. Verify that patient medical record information is released only as permitted under the hospital’s policies and procedures.

5. Conduct observations and interview staff to determine what safeguards are in place or precautions are taken to prevent unauthorized persons from gaining physical access or electronic access to information in patient records.

6. If the hospital uses electronic patient records, is access to patient records controlled through standard measures, such as business

**DOCUMENT REVIEW, INTERVIEW AND OBSERVATION**

1. Verify that policies are in place that limits access to, and disclosure of, medical records to permitted users and uses, and that require written authorization for other disclosures. Are the policies consistent with the regulatory requirements?

2. Observe whether patient records are secured from unauthorized access at all times and in all locations.

3. Ask the hospital to demonstrate what precautions are taken to prevent physical or electronic altering of content previously entered into a patient record, or to prevent unauthorized disposal of patient records.

This standard is not met as evidenced by:

© 2018 HFAP
<table>
<thead>
<tr>
<th>STANDARD / ELEMENT</th>
<th>EXPLANATION</th>
<th>SCORING PROCEDURE</th>
<th>SCORE</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Competency assurance activities, conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs;</td>
<td></td>
<td>rules defining permitted access, passwords, etc.?</td>
<td></td>
</tr>
<tr>
<td>• Business planning, development, management, and administration and certain hospital-specific fundraising activities.</td>
<td></td>
<td>7. Do the hospital’s policies and procedures provide that “original” medical records are retained, unless their release is mandated under Federal or State law, court order or subpoena? Interview staff responsible for medical records to determine if they are aware of the limitations on release of “original” medical records.</td>
<td></td>
</tr>
<tr>
<td><strong>POLICIES AND PROCEDURES</strong></td>
<td>The hospital must develop policies and procedures that reasonably limit disclosures of information contained in the patient’s medical record to the minimum disclosure necessary, except when the disclosure is for treatment or payment purposes, or as otherwise required by State or Federal law.</td>
<td>8. Observe the hospital’s security practices for patient records. Are patient records left unsecured or unattended? Are patient records unsecured or unattended in hallways, patient rooms, nurse’s stations, or on counters where unauthorized persons could gain access to patient records?</td>
<td></td>
</tr>
<tr>
<td>When the minimum necessary standard is applied, a hospital may not disclose the entire medical record for a particular purpose, unless it can specifically justify that the whole record is the disclosure amount reasonably required for the purpose.</td>
<td>9. Verify that there is an established system in place that addresses protecting the confidentiality of medical information.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A hospital may disclose information from the medical record electronically, and may also share an electronic medical record system with other health care facilities, physicians and practitioners, so long as the system is designed and operated with safeguards that ensure that only authorized disclosures are made.</td>
<td>10. If the hospital uses electronic patient records, are appropriate security safeguards in place? Is access to patient records controlled?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The hospital must obtain written authorization from the patient or the patient’s representative for any other disclosure of medical record information.</td>
<td>11. Verify that adequate precautions are taken to prevent physical or electronic altering, damaging or deletion / destruction of patient records or information in patient records.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
PREVENTING UNAUTHORIZED ACCESS
The hospital must ensure that unauthorized individuals cannot gain access to patient records. This applies to records in electronic as well as hard copy formats.

Patient records must be secure at all times and in all locations. This includes open patient records for patients who are currently inpatients in the hospital and outpatients in outpatient clinics.

- For hard copy records, techniques such as locked cabinets or file rooms and limiting access to keys or pass codes may be employed.

- For electronic records technical safeguards, such as business rules that limit access based on need to know, passwords, or other control mechanisms must be in place.

When disposing of copies of medical records, physical safeguards might include first shredding documents containing confidential information, taking appropriate steps to erase information from media used to store electronic records, etc.

RELEASE OF ORIGINAL RECORDS
The hospital must not release the original of a medical record that exists in a hard copy, paper version only, unless it is required to do so in response to a court order, a subpoena, or Federal or State laws.

12. Verify the facility does not permit the texting of orders by physicians or other healthcare providers.

13. It is expected that providers will implement procedures/processes that routinely assess the security and integrity of the texting systems/platforms that are being utilized, in order to avoid negative outcomes that could compromise the care of patients.
For electronic records, the hospital must ensure that the media or other mechanism by which the records are stored electronically is not removed in such a way that all or part of the record is deleted from the hospital’s medical record system.

The hospital must have policies and procedures that address how it assures that it retains its “original” medical records, unless their release is mandated by law/court order/subpoena.

Patient records must be secure at all times and in all locations. This includes patient records for patients who are currently inpatients in the hospital as well as outpatients in outpatient clinics.

Policies are in place that address the organization of the medical records service including:

- Confidentiality
- Release of information
- Retention
- Storage
- Security of medical records in all areas of the inpatient and outpatient areas of the organization.

**SECURE SYSTEMS/PLATFORMS**

In order to be compliant with the CoPs, all providers must utilize and maintain systems/platforms that are secure, encrypted, and minimize the risks to patient privacy and confidentiality as per HIPAA regulations and the hospital and CAH CoPs.
<table>
<thead>
<tr>
<th>STANDARD / ELEMENT</th>
<th>EXPLANATION</th>
<th>SCORING PROCEDURE</th>
<th>SCORE</th>
</tr>
</thead>
</table>

It is expected that providers will implement procedures/processes that routinely assess the security and integrity of the texting systems/platforms that are being utilized, in order to avoid negative outcomes that could compromise the care of patients.
### MEDICAL RECORDS – REVISED STANDARD

<table>
<thead>
<tr>
<th>STANDARD / ELEMENT</th>
<th>EXPLANATION</th>
<th>SCORING PROCEDURE</th>
<th>SCORE</th>
</tr>
</thead>
</table>
| **10.01.03 Legible & Complete.** | All patient medical record entries must be legible, complete, dated, timed, and authenticated in written or electronic form by the person responsible for providing or evaluating the service provided, consistent with hospital policies and procedures. | CHART REVIEW
Review a sample of open and closed medical records.
1. Determine whether all medical record entries are legible. Are they clearly written in such a way that they are not likely to be misread or misinterpreted?
2. Determine whether orders, progress notes, nursing notes, or other entries in the medical record are complete.
3. Does the medical record contain sufficient information to identify the patient;
   - To identify the patient
   - Support the diagnosis / condition
   - Justify the care, treatment, and services
   - Document the course and results of care, treatment, and services
   - Promote continuity of care among providers.
4. Determine whether medical record entries are dated, timed, and appropriately authenticated by the person who is responsible for ordering, providing, or evaluating the service provided.
5. Determine whether all orders, including verbal orders, are written in the medical record and signed by the practitioner who is responsible for ordering, providing, or evaluating the service provided. | ☐ 1 = Compliant ☐ 2 = Not Compliant |  |

§482.24(c)(1)
### MEDICAL RECORDS – REVISED STANDARD

<table>
<thead>
<tr>
<th>STANDARD / ELEMENT</th>
<th>EXPLANATION</th>
<th>SCORING PROEDURE</th>
<th>SCORE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>the person responsible for providing or evaluating the service provided.</td>
<td>caring for the patient and who is authorized by hospital policy and in accordance with State law to write orders.</td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>The time and date of each entry (orders, reports, notes, etc.) must be accurately documented.</td>
<td>Determine whether the hospital has a means for verifying signatures, both written and electronic, written initials, codes, and stamps when such are used for authorship identification.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Timing establishes when an order was given, when an activity happened or when an activity is to take place. Timing and dating entries is necessary for patient safety and quality of care.</td>
<td>• For electronic medical records, ask the hospital to demonstrate the security features that maintain the integrity of entries and verification of electronic signatures and authorizations.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Timing and dating of entries establishes a baseline for future actions or assessments and establishes a timeline of events. Many patient interventions or assessments are based on time intervals or timelines of various signs, symptoms, or events. (71 FR §68687)</td>
<td>• Examine the hospital’s policies and procedures for using the system, and determine if documents are being authenticated after they are created.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>The hospital must have a method to establish the identity of the author of each entry. This would include verification of the author of faxed orders / entries or computer entries.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>The hospital must have a method to require that each author takes a specific action to verify that the entry being authenticated is his/her entry or that he/she is responsible for the entry, and that the entry is accurate.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The requirements for dating and timing do not apply to orders or prescriptions that are generated outside of the hospital until they are presented to the hospital at the time of service. Once the hospital begins</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
processing such an order or prescription, it is responsible for ensuring that the implementation of the order or prescription by the hospital is promptly dated, and timed in the patient’s medical record.

**PRE-PRINTED ORDER SETS**

When a practitioner is using a preprinted order set, the ordering practitioner may be in compliance with the requirement at §482.24(c)(1) to date, time, and authenticate an order if the practitioner accomplishes the following:

1. **Last page:**
   - Sign, date, and time the last page of the orders, with the last page also identifying the total number of pages in the order set.

2. **Pages with Internal Selections:**
   - Sign or initial any other (internal) pages of the order set where selections or changes have been made.
     - The practitioner should initial / sign the top or bottom of the pertinent page(s); and
     - The practitioner should also initial each place in the preprinted order set where changes, such as additions, deletions, or strike-outs of components that do not apply, have been made.
     - It is not necessary to initial every preprinted box that is checked to indicate selection of an
order option, so long as there are no changes made to the option(s) selected.

PRE-ESTABLISHED ELECTRONIC ORDER SET
In the case of a pre-established electronic order set, the same principles would apply, so that the practitioner would date, time and authenticate the final order that resulted from the electronic selection / annotation process, with the exception that pages with internal changes would not need to be initialed or signed if they are part of an integrated single electronic document.

1. Authentication of medical record entries may include written signatures, initials, computer key, or other code.

2. For authentication, in written or electronic form, a method must be established to identify the author.

3. When rubber stamps or electronic authorizations are used for authentication, the hospital must have policies and procedures to ensure that such stamps or authorizations are used only by the individuals whose signature they represent.

4. There shall be no delegation of stamps or authentication codes to another individual. It should be noted that some insurers and other payers may have a policy prohibiting the use of rubber stamps as a means of authenticating the medical records that support a claim for payment.
<table>
<thead>
<tr>
<th>STANDARD / ELEMENT</th>
<th>EXPLANATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Medicare payment policy, for example, no longer permits such use of rubber stamps. Thus, while the use of a rubber stamp for signature authentication is not prohibited under the CoPs and analysis of the rubber stamp method per se is not an element of the survey process, hospitals may wish to eliminate their usage in order to avoid denial of claims for payment.</td>
<td></td>
</tr>
</tbody>
</table>

**Electronic Medical Record**
Where an electronic medical record is in use, the hospital must demonstrate how it prevents alterations of record entries after they have been authenticated. Information needed to review an electronic medical record, including pertinent codes and security features, must be readily available to surveyors to permit their review of sampled medical records while on-site in the hospital.

**Countersignature**
When State law and/or hospital policy requires that entries in the medical record made by residents or non-physicians be countersigned by supervisory or attending medical staff members, then the medical staff rules and regulations must address countersignature requirements and processes.

**Auto-authentication**
A system of auto-authentication in which a physician or other practitioner authenticates an entry that he or she cannot review, e.g., because it has not yet been transcribed, or the electronic entry cannot be
displayed, is not consistent with these requirements.

- There must be a method of determining that the practitioner did, in fact, authenticate the entry after it was created.

- In addition, failure to disapprove an entry within a specific time period is not acceptable as authentication.

The practitioner must separately date and time his/her signature authenticating an entry, even though there may already be a date and time on the document, since the latter may not reflect when the entry was authenticated.

For certain electronically-generated documents, where the date and time that the physician reviewed the electronic transcription is automatically printed on the document, the requirements of this section would be satisfied. However, if the electronically-generated document only prints the date and time that an event occurred (e.g., EKG printouts, lab results, etc.) and does not print the date and time that the practitioner actually reviewed the document, then the practitioner must either authenticate, date, and time this document itself or incorporate an acknowledgment that the document was reviewed into another document (such as the H&P, a progress note, etc.), which would then be authenticated, dated, and timed by the practitioner.

**Computerized Provider Order Entry (CPOE) is the preferred method of order entry by a provider. CMS**
### MEDICAL RECORDS – REVISED STANDARD

<table>
<thead>
<tr>
<th>STANDARD / ELEMENT</th>
<th>EXPLANATION</th>
<th>SCORING PROCEDURE</th>
<th>SCORE</th>
</tr>
</thead>
</table>

has held to the long standing practice that a physician or Licensed Independent Practitioner (LIP) should enter orders into the medical record via a handwritten order or via CPOE.

An order if entered via CPOE, with an immediate download into the provider’s electronic health records (EHR), is permitted as the order would be dated, timed, authenticated, and promptly placed in the medical record.