This decision table is intended to assist providers and others who use electronic health records (EHRs) to become more familiar with common EHR software tools and features. This decision table also helps providers and others to ensure appropriate use of these features to preserve documentation integrity and prevent fraud, waste, abuse, and improper payments. The decision table includes the following columns:

- **EHR Features and Capabilities**: Describes the features within the EHR system and its capabilities;
- **Program Integrity Issue**: Describes potential program integrity issues that can result from inappropriate use of EHR features and capabilities;
- **Recommendations to Ensure Proper Use**: Outlines recommendations to ensure proper use of EHR system features and capabilities; and
- **Best Practices**: Examples of best practices that providers should consider when using EHRs.

Providers and others should review the information in the table and consider implementing the recommendations and best practices to protect the integrity of EHR documentation.
### Table 1. EHR Proper Use Decision Table

<table>
<thead>
<tr>
<th>EHR Features and Capabilities</th>
<th>Program Integrity Issue</th>
<th>Recommendations to Ensure Proper Use</th>
<th>Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Copy and Paste (also referred to as cloning, cookie cutter, copy forward, and cut and paste)</strong></td>
<td>Copy and paste or cloning can lead to redundant and inaccurate information in EHRs. Using this feature can cause authorship integrity issues since documentation cannot be tracked to the original source.[2] Cloned documentation lacks the patient-specific information necessary to support services rendered to each patient. This can affect the quality of care and can cause improper payments due to:</td>
<td>When creating a policy for copy and paste, providers should weigh efficiency against the potential for inaccurate, fraudulent, or unmanageable documentation.[3] Policy should require the provider to modify copied information to be patient-specific and related to the current visit. Policy should control and limit the use of the copy and paste function. Copied information should include proper notation and clear attribution.[4] Policy should make clear that cut and paste should never be used as it changes the original source material.[5] Monitor and audit copy and paste usage in the EHR.</td>
<td>Providers must recognize each encounter as a stand-alone record, and ensure the documentation for that encounter reflects the level of service actually provided and meets payer requirements for billing and reimbursement.[6] Each entry not solely authored by the user must be validated in a manner similar to bibliographic notations and include the name, date, time, and source of the data. This can be satisfied by system software design that routinely provides validation.[7]</td>
</tr>
<tr>
<td>• Enables the user to assume the content of another person’s entry, (for example, by copying forward vital signs)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Replicates information from the previous visit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Selects data from an original or previous source to reproduce in another location</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cut and Paste:</strong> Removes or deletes the original source text or data to place in another location[1]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EHR Features and Capabilities</td>
<td>Program Integrity Issue</td>
<td>Recommendations to Ensure Proper Use</td>
<td>Best Practices</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Populating via Default</strong></td>
<td>Populating via default may encourage over-documentation to meet reimbursement requirements, even when services are not medically necessary or are never delivered.[9] It may also cause upcoding (higher level of service than provided).</td>
<td>Providers should avoid the generation of a note that does not require some action on the part of the provider. Policy should require the provider to review and edit all defaulted data to ensure that only patient-specific data for that visit is recorded. The provider should verify the validity of auto-populated information on entry and delete all irrelevant and unnecessary auto-populated information. Providers should incorporate policies and control structures that require the addition of free text when auto-population methods are used.[10]</td>
<td>None to report at this time.</td>
</tr>
<tr>
<td><strong>Macro</strong></td>
<td>Documentation can be produced for services not rendered, which can lead to over-documentation and upcoding.</td>
<td>Policy should require the provider to verify the validity of information on entry. Providers should incorporate policies and control structures that require the addition of free text when auto-population methods are used.[13]</td>
<td>None to report at this time.</td>
</tr>
<tr>
<td>EHR Features and Capabilities</td>
<td>Program Integrity Issue</td>
<td>Recommendations to Ensure Proper Use</td>
<td>Best Practices</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------</td>
<td>--------------------------------------</td>
<td>----------------</td>
</tr>
</tbody>
</table>
| **Template**  
Documentation tools that feature predefined text and text options used to document the patient visit within a note.[14]  
Use of templates may expose a physician to liability for false claims as the additional documentation may lead to upcoding.  
Problems can occur if the structure of the note is not a good clinical fit and does not accurately reflect the patient’s condition and services.[15]  
Templates may encourage over-documentation to meet reimbursement requirements even when services are not medically necessary or are never delivered.[16]  
Policy should require the use of “open-ended” templates to allow the physician to check boxes for population of some general information.  
Policy should also require the physician to provide additional information to describe the patient in the specific episode of illness.[17]  
Policy should require providers to modify templates so that documentation clearly reflects specific conditions and observations unique to the service, and to clearly identify the services provided.  
The provider must understand the necessity of reviewing and editing all defaulted data to ensure that only patient-specific data for that visit is recorded, while all other irrelevant data pulled in by the default template is removed.[18] |
| **Automated Change of Note Author**  
Automatically changing authorship of a note written by someone else to the current user of the note.  
It may be impossible to verify the actual service provider or the work performed by each provider.  
Providers and others should adopt EHR systems that allow more than one individual to add text to the same progress note entry or flow sheet, while preserving the attribution of each entry to the correct individual. This will enable multiple providers to document and sign, making it possible to verify the actual service provider or the amount of work performed by each provider.  
When there are multiple authors or contributors to a document, all signatures should be retained so that each individual’s contribution is unambiguously identified.[19] |
<table>
<thead>
<tr>
<th>EHR Features and Capabilities</th>
<th>Program Integrity Issue</th>
<th>Recommendations to Ensure Proper Use</th>
<th>Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Audit Trail</strong></td>
<td>EHR system security features, such as the audit log, access restrictions, and warnings can be turned off, which can result in an inadequate and incomplete audit trail.</td>
<td>The HIPAA Security Rule, 45 C.F.R § 164.312(b), mandates that the audit trail be maintained within the EHR. The U.S. Department of Health and Human Services, Office of Inspector General (HHS-OIG) has stated that the EHR system’s audit log should always be turned on.[21] Policy must require that the EHR system audit log remain operational. The only exception is for system performance fixes, updates, stability, and disaster recovery, and only then by an authorized administrator.[22]</td>
<td>The provider may use the audit trail functionality of the EHR system to identify and trend use of health record.[23]</td>
</tr>
</tbody>
</table>

**Dictation/Voice to Text**

The provider dictates notes to a recorder or scribe, or uses voice-to-text software for documenting the patient visit.

Documentation entered in to the EHR by others, through a scribe, through dictated notes, or through voice-to-text software, may not accurately identify or support the need for services provided. Nonvalidation of documentation entered by others may not support claims submitted.

Policy should require providers to review, edit, and approve by signature, any information entered in to the EHR on their behalf (scribes, residents, nurses) in a timely manner.[24, 25]

Organizations have policies and procedures in place to ensure providers review, edit, and approve dictated information in a timely manner.[26]
By understanding the proper use of EHR system features and capabilities, providers and others can ensure integrity in documentation and protect EHR program integrity. Implementing recommendations and best practices outlined in the decision table will help to reduce fraud, waste, abuse, and improper payments with EHR use.

To see the electronic version of this decision table and the other products included in the “Electronic Health Records” Toolkit, visit the Medicaid Program Integrity Education page at http://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/edmic-landing.html on the Centers for Medicare & Medicaid Services (CMS) website.

Follow us on Twitter #MedicaidIntegrity

References


Disclaimer

This decision table was current at the time it was published or uploaded onto the web. Medicaid and Medicare policies change frequently so links to the source documents have been provided within the document for your reference.

This decision table was prepared as a service to the public and is not intended to grant rights or impose obligations. This decision table may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. Use of this material is voluntary. Inclusion of a link does not constitute CMS endorsement of the material. We encourage readers to review the specific statutes, regulations, and other interpretive materials for a full and accurate statement of their contents.

July 2015