UM 12: UM System Controls

The organization has UM system controls to protect data from being altered outside of prescribed protocols.

Intent

The organization develops policies and procedures and conducts audits for system controls specific to UM denial and appeal notification and receipt dates.

Element A: UM Denial System Controls - Existing Requirement

The organization has policies and procedures describing its system controls specific to UM denial notification dates that:

1. **Define the date of receipt consistent with NCQA requirements.**
2. **Define the date of written notification consistent with NCQA requirements.**
3. **Describe the process for recording dates in systems.**
4. **Specify staff who are authorized to modify dates once initially recorded and circumstances when modification is appropriate.**
5. **Specify how the system tracks modified dates.**
6. **Describe system security controls in place to protect dates ~~data~~ from unauthorized modification.**
7. **Describe how the organization audits the processes and procedures in factors 1-6.**

Scoring

Met	Partially Met	Not Met
The organization meets 7 factors	No scoring option	The organization meets 0-6 factors

Data source Documented process, Materials

Scope of review

Product lines

This element applies to all product lines for Interim Surveys, First Surveys and Renewal Surveys.

Documentation

NCQA reviews the organization's policies and procedures for its UM denial system security controls. If the organization outsources storage of UM data ~~information~~ to ~~an~~ external ~~entity~~ entities, NCQA also reviews ~~the contract~~ contracts from up to four randomly selected ~~between the organization and the~~ external ~~entity~~ entities. External entities include data storage providers for the organization's UM data and UM delegates that store their own data. The score for the element is the average of the scores for all external entities.

Look-back period

For All Surveys: ~~Prior to the survey date.~~ *Six months*.

Explanation

~~**THIS IS A MUST PASS ELEMENT.**~~

This element is a **structural requirement.** The organization must present its own documentation.

This element applies to the systems used to manage UM medical necessity decisions in scope of UM 5: Timeliness of UM Decisions.

Factors 1–3

No additional explanation.

***Factor 4:* Authorization to modify dates**

The organization's policies and procedures identify the:

- Level of staff who are authorized to modify dates.
- Circumstances when modification is appropriate.

***Factor 5:* Tracking modifications**

The organization's policies and procedures describe how the system tracks:

- What modification was made.
- When the date was modified.
- The staff who made the modification.
- Why the date was modified.

***Factor 6:* Securing system ~~data~~ dates**

The organization's policies and procedures describe the process for:

- Limiting physical access to the system.
- Preventing unauthorized access and changes to system data.
- Password-protecting electronic systems, including requirements to:
  - Use strong passwords.
  - Avoid writing down passwords.
  - Use different passwords for different accounts.
  - Change passwords periodically.
- Changing or withdrawing passwords, including alerting appropriate staff who oversee computer security to:
  - Change passwords when appropriate.
  - Disable or remove passwords of employees who leave the organization.
- Incident management:
  - Identifying and responding to instances when policies and procedures for securing dates are not being followed.
  - Mitigating, to the extent practical, harmful effects of unauthorized date changes.
  - Documenting and reporting these incidents and their outcome.

If the organization contracts with an external entity to outsource storage of UM data, the contract describes how the contracted entity ensures the security of the data.

Factor 7: **UM controls audit process**

The policies and procedures describe the organization's audit process for identifying and assessing and ensuring that specified policies and procedures are followed. At a minimum, the description includes:

- The audit methodology used, including sampling, the individuals involved in the audit and the audit frequency.
- Oversight of the department responsible for the audit.

Exceptions *None.*

Examples *None.*

Element B: UM Denial Controls Oversight and Audit - NEW

At least quarterly, the organization audits its UM denial controls by:

1. **Analyzing all changes to date entries, including reasons for the change.**
2. **Analyzing instances date changes that did not meet the modification criteria.**
3. **Taking action based on findings in factors 1 and 2.**

Scoring

Met	Partially Met	Not Met
The organization meets 4 factors	No scoring option	The organization meets 0-3 factors

Data source Reports

Scope of review

Product lines

This element applies to all product lines for First Surveys and Renewal Surveys.

Documentation

For First and Renewal Surveys, NCQA also reviews the organization's audit analysis report.

If the organization outsources storage of UM data to external entities, NCQA also reviews contracts and documentation from up four randomly selected external entities. External entities include data storage providers for the organization's UM data and UM delegates that store their own data. The score for the element is the average of the scores for all external entities.

Look-back period **For All Surveys: Prior to the survey date.**

Explanation **THIS IS A MUST PASS ELEMENT.**

This element is a **structural requirement.** The organization must present its own documentation.

This element applies to the systems used to manage UM medical necessity decisions in scope of UM 5: Timeliness of UM Decisions.

Factor 1: All changes to date entries

The organization conducts a qualitative and quantitative analysis of all changes made to UM date entries. The organization's report includes a summary of the total volume of date changes and categorizes the changes by reason. The organization may use reason codes as defined by the organization to categorize the date changes. The organization should not identify staff names or case numbers in the report.

***Factor 2:* Changes that did not meet the modification criteria**

The organization tracks and trends date changes that did not meet its policies and procedures as outlined in UM 12, Element A: UM Denial System Controls. The organization conducts a qualitative analysis and presents its findings via a report.

Factor 3: Actions

The organization documents mitigation steps it has taken or plans to take to address findings from factors 1 and 2. An action may be used to address more than one area of the audit findings.

Element C: UM Appeal System Controls – Existing Requirement

The organization has policies and procedures describing its system controls specific to UM appeal dates that:

1. **Define the date of receipt consistent with NCQA requirements.**
2. **Define the date of written notification consistent with NCQA requirements.**
3. **Describe the process for recording dates in systems.**
4. **Specify staff who are authorized to modify dates once initially recorded and circumstances when modification is appropriate.**
5. **Specify how the system tracks modified dates.**
6. **Describe system security controls in place to protect dates ~~data~~ from unauthorized modification.**
7. **Describe how the organization audits the processes and procedures in factors 1-6.**

Scoring

Met	Partially Met	Not Met
The organization meets 7 factors	No scoring option	The organization meets 0-6 factors

Data source Documented process, Materials

Scope of review

Product lines

Factors 1-6 apply to all product lines for Interim Surveys, First Surveys and Renewal Surveys.

Factor 7 applies to all product lines for Interim Surveys and Frist and.

Documentation

NCQA reviews the organization's policies and procedures for its UM appeal system security controls. If the organization outsources storage of UM data ~~information~~ to ~~an~~ external ~~entity~~ entities, NCQA also reviews ~~the contract~~ contracts from up to four randomly selected ~~between the organization and the~~ external ~~entity~~ entities. External entities include data storage providers for the organization's UM data and UM delegates that store their own data. The score for the element is the average of the scores for all external entities.

Look-back period *For All Surveys:* ~~Prior to the survey date~~ Six months.

Explanation ~~**THIS IS A MUST PASS ELEMENT.**~~

This element is a **structural requirement.** The organization must present its own documentation.

This element applies to the systems used to manage UM medical necessity decisions in scope of *UM 8: Policies for Appeals* and *UM 9: Appropriate Handling of Appeals.*

Factors 1–3

No additional explanation.

***Factor 4:* Authorization to modify dates**

The organization's policies and procedures identify the:

- Level of staff who are authorized to modify dates.
- Circumstances when modification is appropriate.

***Factor 5:* Tracking modifications**

The organization's policies and procedures describe how the system tracks:

- What modification was made.
- When the date was modified.
- The staff how made the modification.
- Why the date was modified.

***Factor 6:* Securing system data**

The organization's policies and procedures describe the process for:

- Limiting physical access to the system.

- Preventing unauthorized access and changes to system data.
- Password-protecting electronic systems, including requirements to:
  - Use strong passwords.
  - Avoid writing down passwords.
  - Use different passwords for different accounts.
  - Change passwords periodically.

- Changing or withdrawing passwords, including alerting appropriate staff who oversee computer security to:
  - Change passwords when appropriate.
  - Disable or remove passwords of employees who leave the organization.
- Incident management:
  - Identifying and responding to instances when policies and procedures for securing dates are not being followed.
  - Mitigating, to the extent practical, harmful effects of unauthorized date changes.
  - Documenting and reporting these incidents and their outcome.

If the organization contracts with an external entity to outsource UM activities, the contract describes how the contracted entity ensures the security of the data.

Factor 7: **UM process audit**

The policies and procedures describe the organization's audit process for identifying and assessing and ensuring that specified policies and procedures are followed. At a minimum, the description includes:

- The audit methodology used, including sampling, the individuals involved in the audit and the audit frequency.
- Oversight of the department responsible for the audit.

Examples *None.*

Element D: UM Appeal Controls Oversight and Audit - NEW

At least quarterly, the organization audits its UM appeal controls by:

1. **Analyzing all changes to date entries, including reasons for the change.**
2. **Analyzing instances date changes that did not meet the modification criteria.**
3. **Taking action based on findings in factors 1-3.**

Scoring

Met	Partially Met	Not Met
The organization meets 3 factors	No scoring option	The organization meets 0-2 factors

Data source Reports

Scope of review

Product lines

This element applies to all product lines for Surveys and First Surveys and Renewal Surveys.

Documentation

For First and Renewal Surveys, NCQA reviews the organization's audit analysis report.

If the organization outsources storage of UM data to external entities, NCQA also reviews contracts and documentation from up four randomly selected external entities. External entities include data storage providers for the organization's UM data and UM delegates that store their own data. The score for the element is the average of the scores for all external entities.

Look-back period

For All Surveys: Prior to the survey date.

Explanation:

Factor 1: All changes to date entries

The organization conducts a qualitative and quantitative analysis of all changes made to UM date entries. The organization's report includes a summary of the total volume of date changes and categorizes the changes by reason. The organization may use reason codes as defined by the organization to categorize the date changes. The organization should not identify staff names or case numbers in the report.

***Factor 2: C*hanges that did not meet the modification criteria**

The organization tracks and trends date changes that did not meet its policies and procedures as outlined in UM 12, Element A: UM Denial System Controls. The organization conducts a qualitative analysis and presents its findings via a report.

Factor 3: Actions

The organization documents mitigation steps it has taken or plans to take to address findings from factors 1 and 2. An action may be used to address more than one area of the audit findings.

CR 1: Credentialing Policies

The organization has a well-defined credentialing and recredentialing process for evaluating and selecting licensed independent practitioners to provide care to its members.

Intent

The organization has a rigorous process to select and evaluate practitioners.

Element C: Credentialing System Controls– Existing Requirement

The organization's credentialing process describes:

1. **How primary source verification information is received, dated and stored.**
2. **How modified information is tracked and dated from its initial verification.**
3. **Staff who are authorized to review, modify and delete information, and circumstances when modification or deletion is appropriate.**
4. **The security controls in place to protect the information from unauthorized modification.**
5. **How the organization audits the processes and procedures in factors 1–4.**

Scoring

Met	Partially Met	Not Met
The organization meets 5 factors	No scoring option	The organization meets 0-4 factors

Data source Documented process, Materials

Scope of review

Product lines

This element applies to all product lines for Interim Surveys, First Surveys and Renewal Surveys.

Documentation

NCQA reviews the organization's policies and procedures for its CR system security controls. If the organization outsources storage of credentialing ~~information~~ data to ~~an~~ external ~~entity~~ entities, NCQA also reviews ~~the contract~~ contracts ~~between the organization and the~~ from up to four randomly selected external ~~entity~~ entities. External entities include data storage providers for the organization's CR data and CR delegates that store their own data. The score for the element is the average of the scores for all external entities.

Look-back period *For Interim Surveys, First Surveys and Renewal Surveys:* ~~Prior to the survey date~~ Six months.

Explanation ~~**THIS IS A MUST-PASS ELEMENT.**~~

This element is a **structural requirement.** The organization must present its own documentation.

This element applies to both paper and electronic credentialing processes.

Factor 1: **Primary source verification information**

The organization's policies and procedures describe how credentialing information is received, stored, reviewed, tracked and dated.

Factor 2: **Tracking modifications**

The organization's policies and procedures describe how it tracks:

- Modifications made to credentialing information:
  - When the information was modified.
  - How the information was modified.
  - Staff who made the modification.
  - Why the information was modified.

Factor 3: **Authorization to modify information**

The organization's policies and procedures identify the:

- Level of staff who are authorized to access, modify and delete information.
- Circumstances when modification or deletion is appropriate.

Factor 4: **Securing information**

The organization's policies and procedures describe the process for:

- Limiting physical access to credentialing information, to protect the accuracy of information gathered from primary sources and NCQA-approved sources.
- Preventing unauthorized access, changes to and release of credentialing information.
- Password-protecting electronic systems, including user requirements to:
  - Use strong passwords.
  - Avoid writing down passwords.
  - Use different passwords for different accounts.
  - Change passwords periodically.
- Changing or withdrawing passwords, including alerting appropriate staff who oversee computer security to:
  - Change passwords when appropriate.
  - Disable or remove passwords of employees who leave the organization.
- Incident management:
  - Identifying and responding to instances when policies and procedures for securing dates are not being followed.
  - Mitigating, to the extent practical, harmful effects of unauthorized date changes.
  - Documenting and reporting these incidents and their outcome.

If the organization contracts with an external entity to outsource storage of credentialing information, the contract describes how the contracted entity ensures the security of the stored information.

Factor 5: **Credentialing process audit**

The policies and procedures describe the organization's audit process for identifying and assessing risks and ensuring that specified policies and procedures are followed. At a minimum, the description includes:

- The audit methodology used, including sampling, the individuals involved in the audit and the audit frequency.
- Oversight of the department responsible for the audit.

Exceptions

None.

Examples None.

Element D: Credentialing Controls Oversight and Audit - NEW

At least quarterly, the organization audits its CR controls by:

1. **Analyzing all changes to date entries, including reasons for the change.**
2. **Analyzing instances date changes that did not meet the modification criteria.**
3. **Taking action based on findings in factors 1 and 2.**

Scoring

Met	Partially Met	Not Met
The organization meets 3 factors	No scoring option	The organization meets 0-2 factors

Data source Documented process, Reports

Scope of review

Product lines

This element applies to all product lines for Interim Surveys, First Surveys and Renewal Surveys.

Documentation

NCQA reviews the organization's audit process in place throughout the look-back period.
For First and Renewal Surveys, NCQA also reviews the organization's audit report.

If the organization outsources storage of credentialing data to external entities, NCQA also reviews contracts and documentation from up four randomly selected external entities. External entities include data storage providers for the organization's CR data and CR delegates that store their own data. The score for the element is the average of the scores for all external entities.

Explanation **THIS IS A MUST PASS ELEMENT.**

This element is a **structural requirement.** The organization must present its own documentation.

This element applies to both paper and electronic credentialing processes.

Factor 1: All changes to date entries

The organization conducts a qualitative and quantitative analysis of all changes made to UM date entries. The organization's report includes a summary of the total volume of date changes and categorizes the changes by reason. The organization may use reason codes as defined by the organization to categorize the date changes. The organization should not identify staff names or case numbers in the report.

***Factor 2: C*hanges that did not meet the modification criteria**

The organization tracks and trends date changes that did not meet its policies and procedures as outlined in UM 12, Element A: UM Denial System Controls. The organization conducts a qualitative analysis and presents its findings via a report.

Factor 3: Actions

The organization documents mitigation steps it has taken or plans to take to address findings from factors 1 and 2. An action may be used to address more than one area of the audit findings.