Protecting the Integrity of UM Denial Information

Executive Sponsor: Chief Medical Officer

Issuing Department: Health Services Management (HSM) – Clinical Management

Gate Keeper: Director, Clinical Management

Compliance Statement:
Enforcement: This Policy and Procedure establishes SummaCare's (Plan) process and procedures for protecting the integrity of UM denial information. The Plan has UM system (Guiding Care) controls to protect data from being altered outside of prescribed protocols. The Plan's procedures for processing UM authorizations (including approvals and denials) describe the process in place to maintain information integrity and security. UM staff adhere to operational procedures for entering data related to Utilization Management requests.
Review Schedule: This policy will be reviewed and updated as necessary and no less than every two years.
Monitoring and Auditing: Thie Issuing/Collaborating Department(s) is responsible for monitoring compliance with this policy.
Documentation: Documentation related to this policy must be maintained for a minimum of 10 years.

APPLIES TO:

☒ SummaCare
☒ Summa Management Service Organization (SMSO)
☒ APEX
☒ Summa Insurance Company

LINE(S) OF BUSINESS:

☒ Commercial Groups
☐ Medicare Supplemental
☒ Off-Exchange
☒ Medicare
☒ On-Exchange
☒ Self-Funded

1.0 Purpose: This Policy and Procedure establishes SummaCare's (Plan) process and procedures describing how the integrity of information in the scope of Utilization Management (UM) information is protected.

2.0 Policy:

2.1 The Plan has UM system (Guiding Care) controls to protect data from being altered outside of prescribed protocols. The Plan's procedures for processing UM authorizations (including approvals and denials) describe the process to maintain information integrity and security. UM staff adhere to operational procedures for entering data related to utilization management requests.

3.0 Procedure:

Definitions:

- **Date of receipt:** The date the Plan receives the request from the member or the member's authorized representative, even if the Plan does not have all the information necessary to make a decision. Also referred to as the receipt date.

- **Date of written notification:** The date when the notice of the UM decision was sent to the member and practitioner as documented on the denial notice. If electronic notification is used, the written notification date is the date the notification was posted in the electronic system. Also referred to as the notification date.

- **Scope of UM information:** UM information includes:

    - UM requests from members or their authorized representatives
    - UM request receipt date
    - Appropriate practitioner review
    - Use of board-certified consultants
    - Clinical information collected and reviewed
    - UM decisions
    - UM decision notification date
    - UM denial notices

3.1 The process for recording dates in Guiding Care consists of auto-generation of date/time stamped by the system when submitted by fax or through the online portal Date Documentation. The request receipt dates are documented and viewable in the UM record.

3.1.1 The system autogenerates the receipt dates based on the date and time of the request either submitted by fax or through the online portal.

3.1.1.1 If the request is faxed, the date and time reflected is the date and time stamp on the fax.

3.1.1.2 If the request was received by mail, the request is date stamped when it is received by the health plan, not when the request was routed to the correct department.

3.1.1.3 If the request was received by phone, the date and time reflected is the date and time of the original telephonic request.

3.1.1.4 If the request was received via the UM system portal (Altruista), the portal automatically date and time stamps the request as of the date and time the request was transmitted to the Plan.

3.1.2 The system automatically records the notification date detail to capture written notification date. The written notification is date and time-stamped by the Guiding Care system. Once the date is automatically generated by the system, it cannot be modified under any circumstance.

3.2 Staff Responsible to Document Completion of UM Activities and Authorization to Modify UM Information

3.2.1 All users can document completion of UM activities. No User can modify or delete notes, clinical information, letters, documents or determinations. A process was put in place to submit a request to one appointed individual to complete the deletion request. Users who can document completion of UM activities and modify UM information include:

3.2.1.1 RN, SNF Coordinators

3.2.1.2 Coordinator, Authorizations and Case Assistant

3.2.1.3 Administrative Assistants Manager; UM Manager; CM Manager; Administrative Services; RN Informatics and Operations; Medical Directors; Chief Medical Officer

3.2.1.4 The UM Manager is responsible for oversight of UM information integrity functions, including auditing.

3.2.2 Date modifications are appropriate under the following circumstances:

3.2.2.1 The incorrect date was entered due to an auto generation or data entry error.

3.2.2.2 The incorrect date was entered because the date stamp on the FAX was incorrect.

Using Guiding Care Authorization Timeliness reports, the UM Discharge Planning/Auditing Nurse or a department manager reviews the report daily for errors. This allows for timely resolution and correction of dates/times that were incorrectly entered.

3.2.3 Tracking Modifications

Guiding Care's Audit Log report includes the following detail:

3.2.3.1 If errors are found, the UM Discharge Planning/Auditing Nurse or Manager sends an email to the appropriate staff member to correct the error.

3.2.3.2 The UM Discharge Planning/Auditing Nurse will go into Guiding Care to see if appropriate correction was made within 3 days of emailing request for correction.

3.2.3.3 If necessary, a second request is sent. If correction is still not completed the Manager, UM will contact staff member to enter correction.

3.2.3.4 Authorization File reports are used to track modifications and accuracy of entries. The History section of the UM record displays why the modification was made that includes, Date and Time of the date modification and username associated with each action.

3.3 Inappropriate Documentation and Updates

3.3.1 The following documentation and updates are inappropriate:

3.3.1.1 Falsifying UM dates (e.g., receipt date, UM decision date, notification date).

3.3.1.2 Creating documents without performing the required activities.

3.3.1.3 Fraudulently altering existing documents (e.g., clinical information, board certified consultant review, denial notices).

3.3.1.4 Attributing review to someone who did not perform the activity (e.g., appropriate practitioner review).

3.3.1.5 Updates to information by unauthorized individuals.

3.4 Securing System Data

Guiding Care data is secured by:

3.4.1 Limiting physical access to the system with:

3.4.1.1 Implementation of user-specific passwords.

3.4.1.2 Utilization of system security for server, hardware, physical records, files and software such as firewalls, intrusion detection systems, logical access control systems and encryption systems.

3.4.1.3 Preventing unapproved software and hardware from being installed on Plan assigned computers by any staff.

3.4.1.4 Using automatic log-off process to automatically log off a Guiding Care user when there has been no activity on a computer terminal/workstation for 30

minutes. Re-establishment of the session may only take place after the user has provided their password.

3.4.2 Preventing unauthorized access and changes to system data:

3.4.2.1 Access is only provided with a completed IT Request for Access form submitted/signed by their appropriate manager.

3.4.2.2 No person shall access, modify or use information systems without authorization and system detection.

3.4.3 Password protecting systems.

3.4.3.1 All staff are required to use a strong password. Passwords must contain at least six letters, four digits and one non-alphabetic character.

3.4.3.2 Passwords cannot be the same as the user ID.

3.4.3.3 User IDs and Passwords are unique to each user.

3.4.3.4 Staff are discouraged from writing down passwords.

3.4.3.5 Staff can use only one login account at a time.

3.4.3.6 Staff are required to change passwords at least once every 90 calendar days or sooner upon request by a supervisor, RN Informatics & Operations, or IT Technical Services or if the password is compromised. Guiding Care Single Sign On automatically prompts users to change their password every 90 calendar days. Staff members can change passwords more frequently if desired by accessing the password change feature.

3.4.3.7 Staff have a maximum of five login attempts before they are locked out and need to be unlocked by the RN, Informatics and Operations nurse or a manager.

3.4.4 The UM Manger or Nurse Informatics RN notifies the SummaCare Help desk to disable or remove passwords when an employee changes positions and no longer requires Guiding Care access or when employment terminates.

3.5 Auditing, Documenting and Reporting Information Integrity Issues

The UM Manager audits UM staff documentation and updates at least annually. If inappropriate modifications are found, the inappropriate modification is documented and reported to the Chief Medical Officer.

If fraud or misconduct is identified the Chief Medical Officer or designee reports to NCQA in accordance with Section 5: Notifying NCQA of Reportable Events. The threshold for reporting to NCQA is self-identification of systemic issues affecting 5% or more of eligible UM files.

Consequences for inappropriate documentation and updates includes one-on-one coaching, departmental education sessions or written corrective action, up to and including, termination of employment.

4.0 Attachments:

4.1 None

5.0 References:

5.1 None

ORIGINAL EFFECTIVE DATE: 11/16/2020
REVIEWED: 7/19/21; 5/17/22, 10/24/2022, 9/25/2025
REVISED: 11/01/22, 5/14/2024, 9/25/2025
APPROVED: 11/21/22, 5/14/2024, 2/12/2026