Solo® Escalation Policies

USER GUIDE

Contents

Copyrights

Patent(s):

https://teladochealth.com/patents/

Last updated: February 2024

Definition of “Device”

Use of the word “device(s)” in this User Guide refers to Teladoc Health telehealth products, not medical devices as defined in Section 201(h) of the Federal Food, Drug, and Cosmetic (FD&C) Act.

In addition, the term “mobile devices” refers to smartphones and tablets.

Virtual Care System

Solo® integrated virtual care platform

Health systems view virtual care as an extension of their services, relying on a combination of software, hardware, networks, systems and people to work together to deliver improved access and care to their patients.

Enabling healthcare's only integrated virtual care platform, Teladoc Health powers virtual encounters at clinics, healthcare facilities and patient homes for an integrated experience across a multitude of use cases. Built on our cloud-based network, Solo® is the backbone to delivering care anywhere at any time. It provides users with everything they need to streamline their telehealth needs for fast user adoption.

Designed for healthcare, security and reliability

Our cloud-based, patented network ensures the industry's highest standards for protecting and securing sensitive healthcare information. Our downloadable and web-based platform allows users to access virtual care across a broad range of consumer and telehealth devices in a variety of clinical environments.

Within a single platform, users are in control of their virtual experience with a configurable dashboard to meet the unique set of preferences for every user. Layer Solo® into your existing health information technology system investments or use it as the foundation to close your workflow gaps with our software modules, creating a solution unique to you.

With Solo, you can connect people, systems, information technology systems, devices, and third-party applications to enable telehealth solutions across patient journeys. Whether launching a scheduled visit, providing care for patients, Solo® provides a core set of tools to deliver virtual care to users with an immersive, patient-centric view of their clinical workflows.

Solo® Care Coordination Overview

This guide is for Emergent Notification Routing and Escalations using Solo®. Solo® is a virtual health care platform that combines detailed intake processes, electronic health records, insurance eligibility checking, online payment, e-prescribing, and video conferencing. Solo® works with your internet browser on any device with a webcam and internet.

TigerConnect and QGenda Feature Overview

Automated User Pairing

When a client admin opens the scheduling or messaging integration pages, Solo® users will be automatically paired with users from the client's scheduling/messaging tool. This automation simplifies the process of managing user relationships and ensures accurate pairing.

Note: If the user used a different email address, or Auto-Merge is otherwise not working, you can make a pair manually. See page 12 for more information on manual pairing.

Scheduling and Messaging Integration

Column displays which integrations each user is configured for. This provides a clear overview of user settings.

Integration pages support the National Provider Identifier (NPI) for pairing users ensuring more accurate and reliable user pairing.

Each user entry on the TigerConnect and QGenda Settings pages includes:

- A date, time and time zone stamp indicating the last time the entry was updated or revised.
- The full name of the user for better identification and management.
- The users email and/or NPI number.

User Tabs separate paired and unpaired users. This allows client admins to easily switch between views and manage users effectively.

Manual User Pairing for TigerConnect and QGenda

Preconditions

- The users exist in the clients TigerConnect and/or QGenda applications.
- The users have been assigned to a task (schedule).
- A Solo® Practitioner Admin or Practice Admin user role is required to pair users.

How to pair users manually

1. Navigate to **Users Profile** > **Practice Settings** > **QGenda Settings** or **TigerConnect Settings**

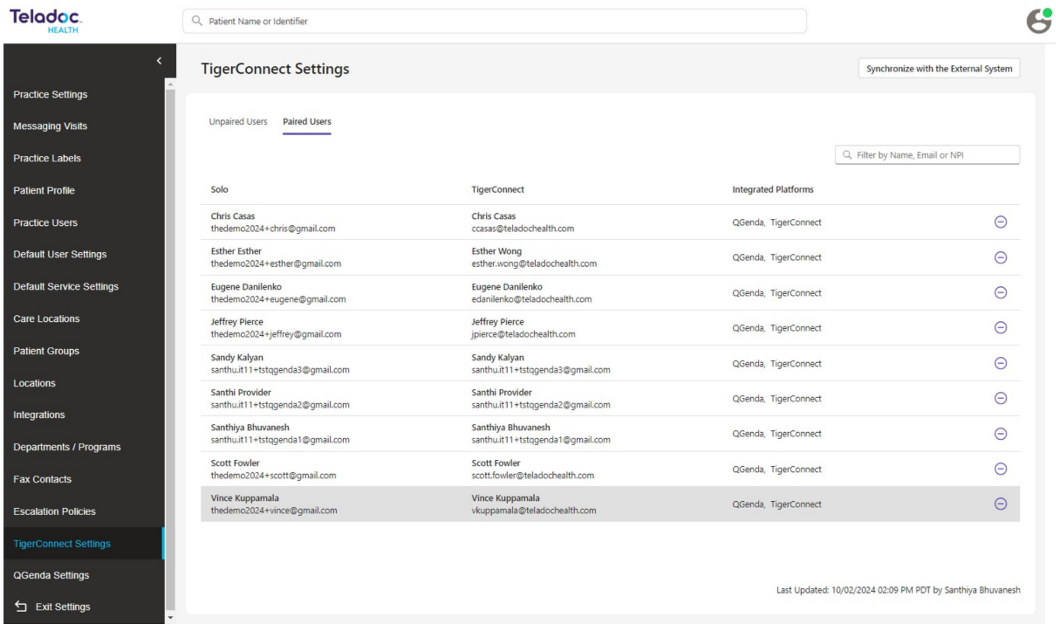
   The integration of Solo® and TigerConnect/QGenda will automatically display users from both applications that have the same unique email address. If the user used a different email address, or Auto-Merge is otherwise not working, you can make a pair manually.

2. Select two users to pair manually > **Pair Manually**

   > NOTE: If a client admin makes a change to their scheduling application, then they can click on "Synchronize with the External System" to manually sync any recent schedule changes. Clients external scheduling application will be automatically synced with Solo® every 10 minutes.

   The Paired users will then be displayed under the "Paired Users" section of the page. The paired user(s) can then be added into an escalation policy/path. See page 15 for more info about escalation policies.

Paired Users Overview



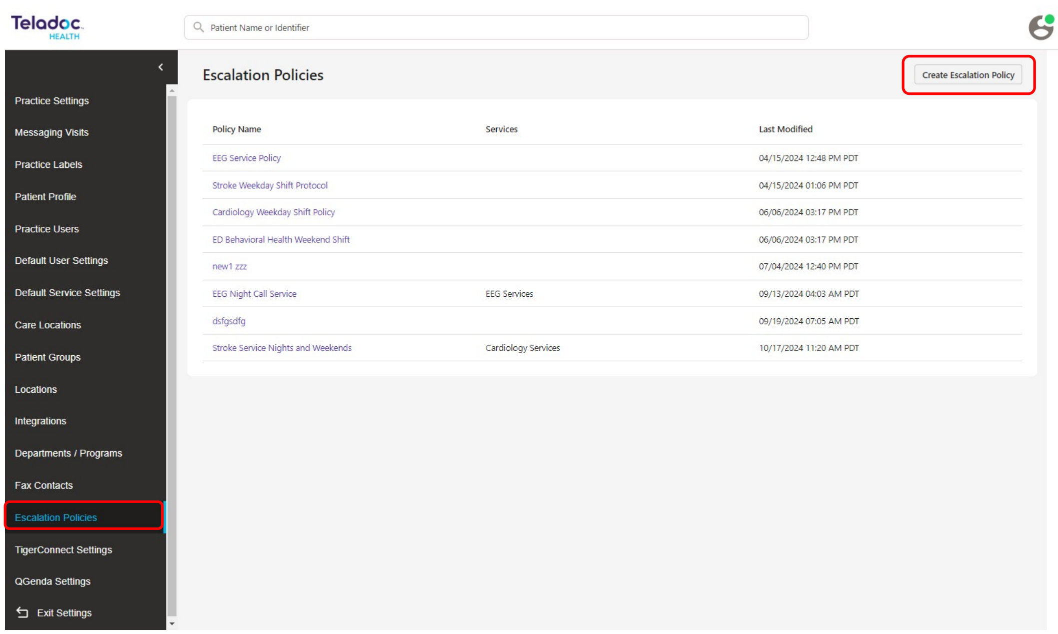
Escalation Policies

Preconditions

- Client must have an integration with their external notification's application.
- Clients must have an integration with their external scheduling application.
- Users must be paired between Solo®, Notifications and Scheduling applications as mentioned above.
- Users must be scheduled in the clients scheduling application.
- A Solo® Practitioner Admin user role is required to pair users.
- Only Emergent encounter-based visit types from the encounter dashboard are supported.
- Only emergent workflows are supported.

Creating an Escalation Policy

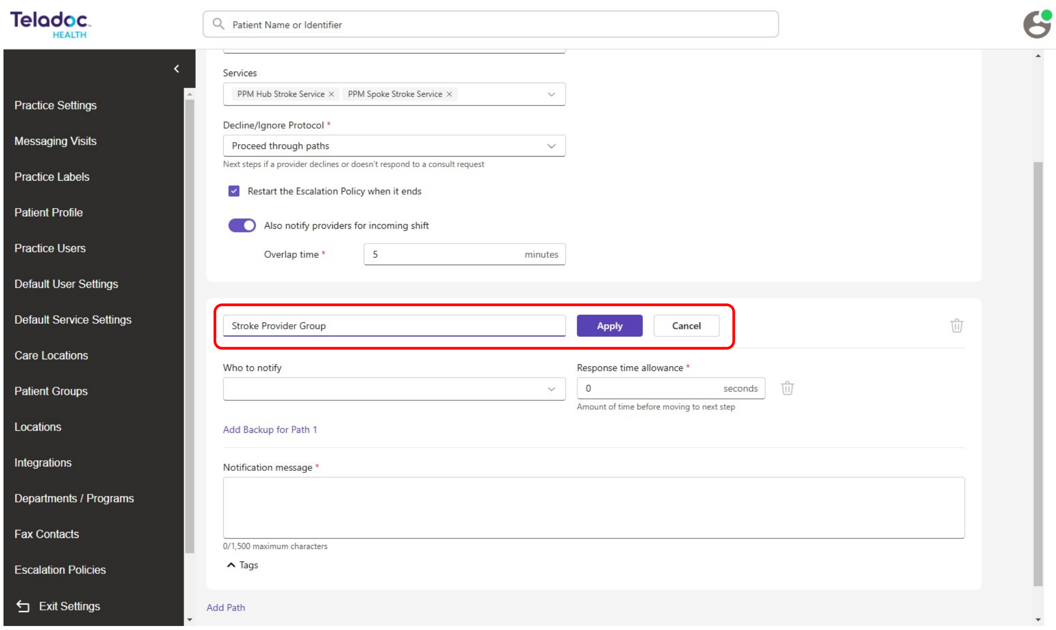
1. Navigate to Users Profile > Practice Settings > Escalation > Create Escalation Policy



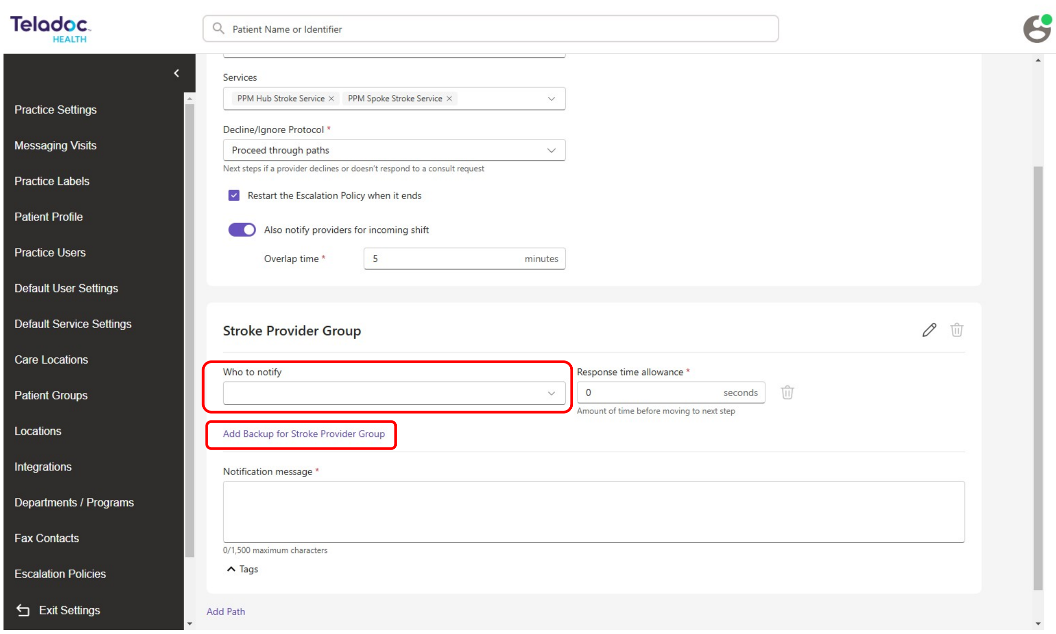
2. In General Settings add:
   - The "Policy Name" of the escalation policy you are adding.

- "Service" associated with the escalation policy.
- Set the "Decline/Ignore Protocol".
- Select if you want to "Restart the escalation policy when it ends".
- Select if you want to "Also notify providers for incoming shifts".

3. Customizing name of Path 1 > Pencil icon > Edit Path 1 name > Apply



4. Add "Who to notify" using the type-ahead in the dropdown.



NOTE

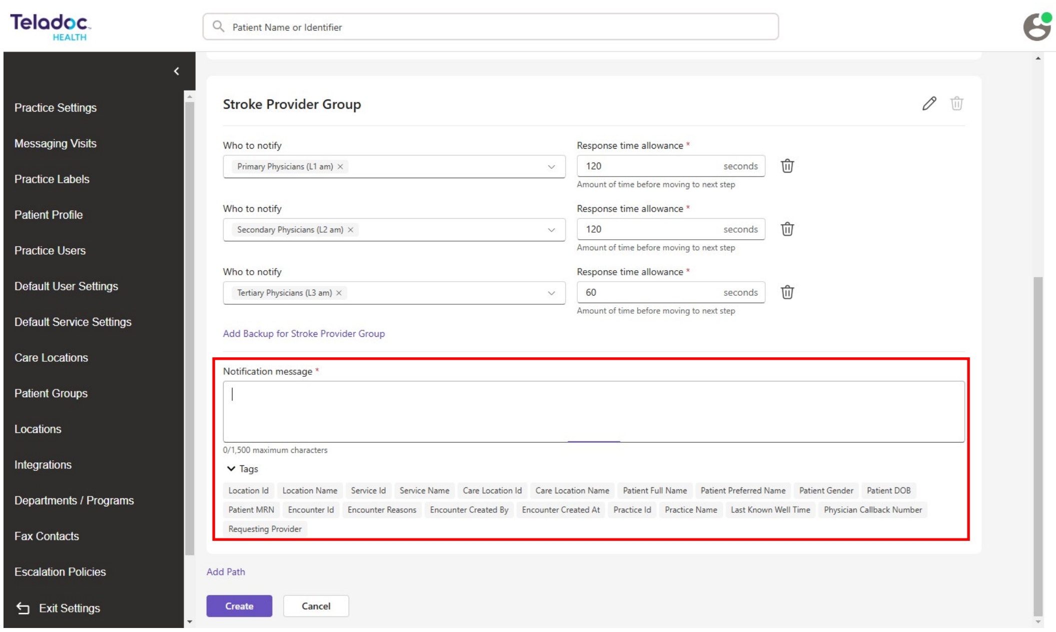
You can create one or multiple "Who to notify" steps in an escalation path. The number of paths is limited to 5 and the number of steps is limited to 10

NOTE
See page 15 for more information on task-syncing with QGenda

5. Add the Response Time Allowance (in minutes), which is the amount of time that elapses before the next step.

NOTE
Clicking on the "Trash" icon will remove the "Who to notify" step.

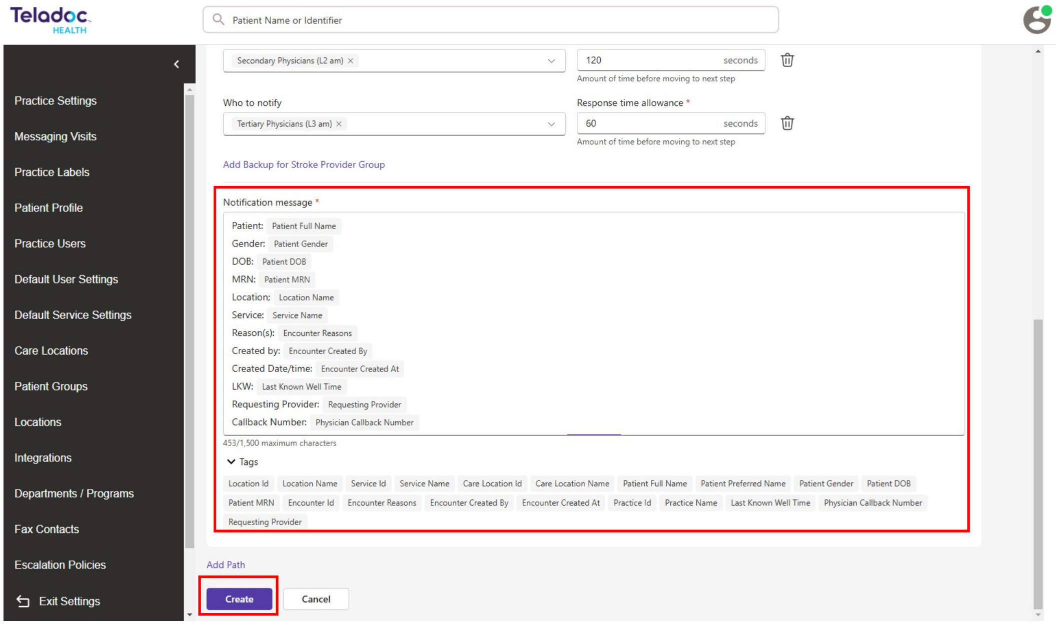
6. Add custom messaging in "Notification Text" by adding available Tags.



NOTE
Make sure all required field denoted by an asterisk (*) are completed prior to the next step

NOTE
See page 16 about adding Smart Note fields as tags to Notification Text

Configured "Notification message" example:



7. Click “Create” to complete the set-up. Click “Cancel” to discontinue creating a new escalation policy and changes will not be saved.

> **NOTE**
> You can create one or multiple escalation paths with different recipients and notification messages

Linear Escalation Policy with Decline/Ignore Protocol

Administrators can configure an escalation policy with Decline/Ignore Protocol set to “Proceed through Paths.” When this protocol is set, the following occurs:

- Instant transition to subsequent steps once a provider declines within the primary Paths.
- Accept and decline buttons maintain visibility across all Path steps in the client messaging tool.
- Parallel processing across multiple paths; a decline in a Path triggers subsequent steps in Path 1 and additionally configured concurrent paths.
- Unaffected continuity for concurrent paths if a user chooses to ignore a step within Path 1.
- Trigger of a new escalation policy step upon user’s decline button action, persisting the button in the UI for reference.
- System-generated browser notification to inform users of consult declination.

Restarting an Escalation Policy after the Policy Ends

An admin can restart the escalation policy from the beginning after it processes the last step. This feature ensures continuous attempts to address consult requests until a practitioner accepts the consult or the maximum cycle limit (10 cycles) is reached.

Escalation Policy Restart Options

Automatic Restart

Once all “Who to notify” steps in an escalation policy have been processed without a practitioner accepting the consult request, the policy will automatically restart from Path 1, “Who to notify” steps.

Immediate Restart

If the last step of the escalation policy is configured with zero-time allowance, the first step will begin immediately after the last step ends.

Configuring Restart Options

A configuration called “Restart the Escalation Policy when it ends” is located under General Settings. A checkbox is located under the Decline/Ignore Protocol options to enable or disable this feature.

> **NOTE**
> The default setting is OFF.
> When ON, the escalation policy will continue to execute, process, and restart for up to 10 cycles.

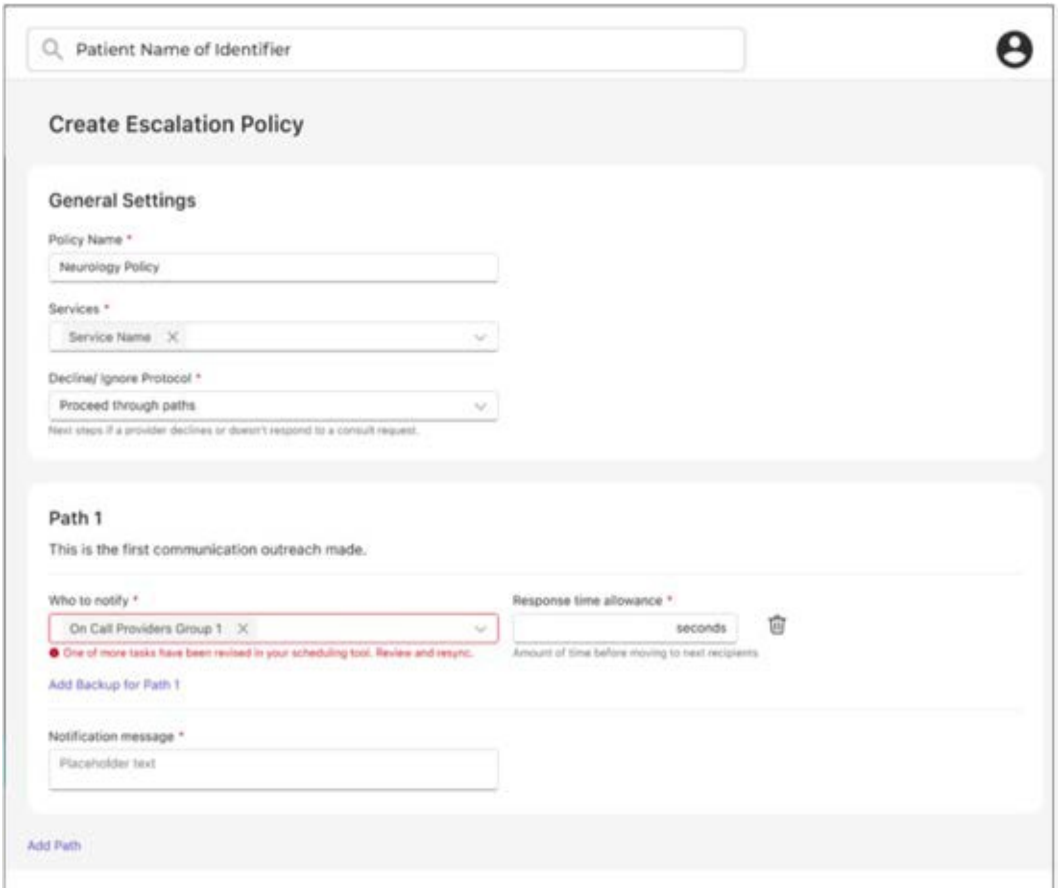
Error Messaging for Unsynchronized Tasks between an Escalation Policy and QGenda

Admins are promptly notified within Solo® when a task synced with Qgenda is deleted or becomes unsynced, enabling swift action to maintain the integrity of escalation policies and uninterrupted notifications.

Upon deletion of a Qgenda-synced task, Solo® will display an error state below the affected step in the corresponding escalation policy.

The error message “One or more tasks have been revised in your scheduling tool. Review and resync.” Alerts administrators to the task deletion, prompting them to take corrective action in Qgenda to avoid disruptions to notifications and potential impacts on patient care.

Error message:



Adding Smart Note fields as tags to Notification Messages

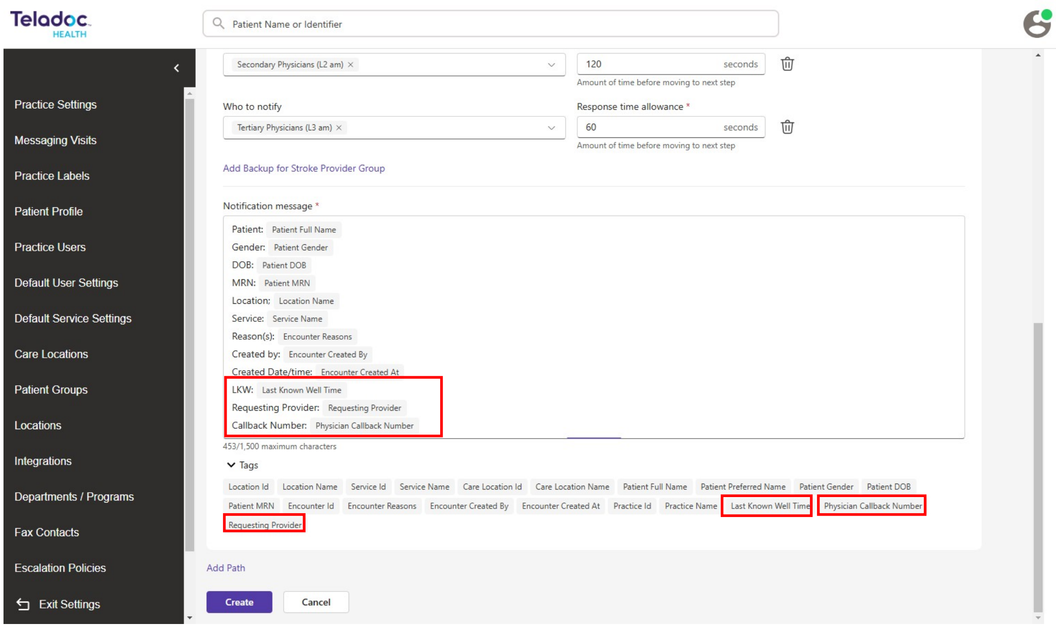
Administrators can incorporate smart notes fields as tags in escalation policy notification messages. This ensures that providers receive comprehensive patient information, empowering them to make informed decisions regarding consult requests. Providers will receive notifications enriched with additional patient information, enabling them to render decisions effectively.

Note about Delayed Tag Application:

- To ensure tagged data is included in notification messages, a 5-second delay is implemented for each consult creation. This accommodates variations in data availability depending on the method of encounter creation.
- If there is a change in the JSON template at the service level, then the tags will disappear from the escalation policy notification messages and will appear blank in the provider's message.

- If a service is removed from an escalation policy, then the then the tags will disappear from the escalation policy notification messages and will appear blank in the provider's message.

There is no error message to indicate tags will be removed from escalation policies if the JSON template is removed from the service.



NOTE

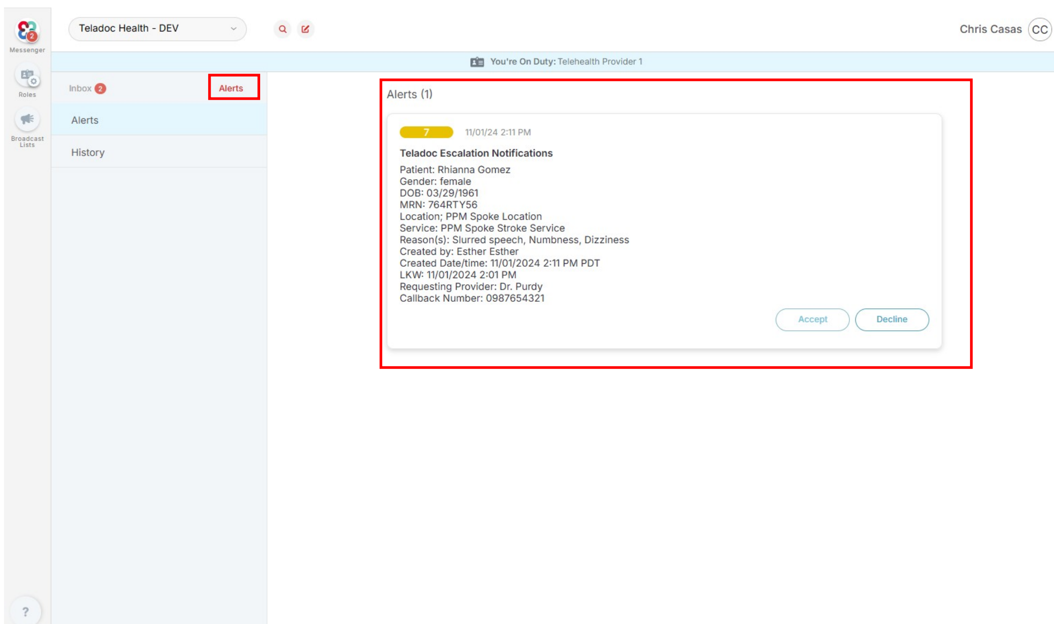
To implement this feature, contact the support team. They will update the JSON templates with the required JSON configurations.

Escalation Process and Execution

Confirming an escalation policy is executed

Preconditions

- A new patient record and encounter were added.
- User(s) were paired across applications (Solo®, QGenda and TigerConnect).
- User(s) were scheduled.
- User(s) received an “Alert” notification in their Messenger.



How it works

Once the user accepts the new consult request in their “Alerts”, a new message will be sent to their “Inbox”, with the Solo® Consult Link. Users can click on the Solo® Consult Link to launch them directly to the consult in the Encounter page.

- **Accepting** a consult stops the configured escalation policies.
- **Declining** a consult immediately notifies the next configured user(s).
- **Ignoring** a consult immediately notifies the next configured user(s).

In General Settings, if a user configures the “Decline/Ignore Protocol” to “Stop

Escalations and Contact Decline Recipients", and a user "Declines" a consult, then the primary paths and steps are stopped, a Decline Path commences (if configured), and recipient(s) are notified.

If the primary user(s) in a configured step "Ignores" the consult, then the secondary user(s) in a configured step are notified.

- If primary and secondary user(s) in configured steps "Ignores" the consult, then confirm the tertiary user(s) in a configured step are notified
- If primary, secondary and tertiary user(s) in configured steps "Ignores" the consult, then the user(s) in the next configured step are notified.

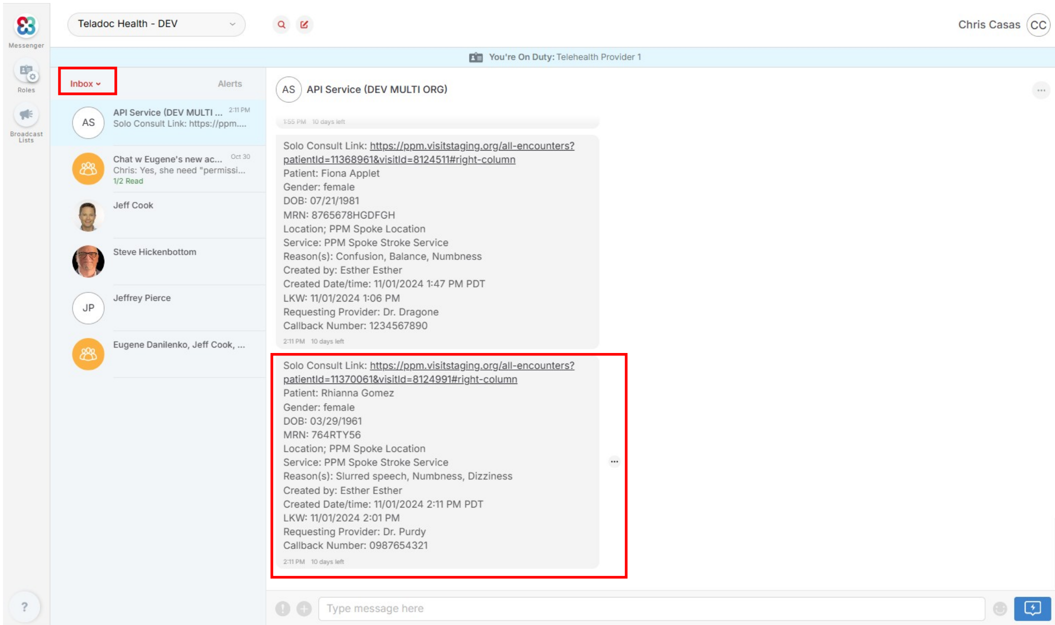
New Consult Follow up Message to Provider in TigerConnect

Providers who accept a new consult request in TigerConnect Messenger will automatically receive a follow-up message in their inbox containing a Solo® Visit URL along with relevant patient information.

After a provider user accepts a consult in their TigerConnect Messenger "Alert Box", they will receive a second message in their "Inbox" (not Alert). The follow-up message will include the same notification text and a URL link to the Solo® consult. Tagged data from the notification message will be included under the URL. The message will be labeled "Solo® Consult Link."

> **NOTE**
> Admins do not need to configure the URL in the notification text. The system will automatically include it in the follow-up message.

Follow-up message example:



Unassigning Provider(s) from a Consult Request

When a provider or another user "unassigns" a previously assigned consult, the consult becomes available to notify other providers in the practice. This ensures consults are efficiently managed and reassigned according to the configured escalation policies.

If unassigned, the configured escalation policy will resume, notifying recipient(s) in the next configured step of the Path according to the policy.

Once all configured steps of the policy are processed, or if there are no other steps configured, the policy will stop after the last step of the path unless the client configures the path to restart.

> **NOTE**
> An escalation policy can be configured to be executed from Path 1 to a Decline Path1.

Encounter Audit Log Events

Assigned Provider events are logged in the encounter audit log, capturing essential data to uphold standards of care, ensure compliance, mitigate risks, and enhance communication and collaboration. This provides admins with real-time access to critical actions, ensuring comprehensive tracking and transparency for consult management.

The following actions are included in the audit log:

- Provider Assigned to a Consult
- Provider Unassigned to a Consult
- Provider Reassigned to a Consult
- Provider Declined a Consult

Solo® Escalation Policy Reporting

Solo® Escalation Policy Reporting data is available through the HHS Data Teams SQL Server Reporting Services (SSRS) (commonly known as the BI Reports Portal). Using this portal, clients can subscribe to data sets on a daily/weekly/monthly basis. The Teladoc Health FleetOps team manages the email subscription services.

This includes new data elements and formats per the Solo® Escalation Policy Data Dictionary, recipient action tracking for each action (accept, decline, ignore, unassign), and a row for each notified recipient. Concurrent consult calculations for newly created, unassigned consults, and time since encounter calculations are also included. Ignored events are excluded but can be reviewed in the encounter audit log or user activity logs. Ignore actions display time since in hh:ss format relating to the response time allowance. Historical data can be applied to new column headers in case of path name changes.

User Activity Log Events

Escalation policy events are in the User Activity Logs (UALs) in Super Admin to enhance tracking and transparency of user actions related to consult management. Detailed logging of key user events provides valuable insights and accountability.

New user events added in User Activity Logs include:

- User accepted (assigned) to a consult, logs when a user accepts and is assigned to a consult.
- User unassigned from a consult, logs when a user is unassigned from a consult.
- User declined a consult, logs when a user declines a consult.
- User Did not respond to a consult, logs when a user does not respond to a consult.

Each event in the User Activity Logs will include the following common data elements:

- Username, the name of the user who took the action.
- User Role, the role of the user within the system.
- Datetime of Action, the date and time when the action occurred.

Configuration and Usage

- The new user events will be visible in the User Activity Logs accessible to Super Admin users.
- These logs will help track and audit user actions related to consult management, improving oversight and operational transparency.

Contact Information

24/7 Live Technical Support

1-877-484-9119

24/7 Live Remote Technical Support & Live Chat

https://teladochealth.com/contact

Email Support

tac@teladochealth.com

Teladoc Health User Manuals

https://solosupport.teladochealth.com

Sales & Product Demos

1-805-562-8686

teladochealth.com | engage@teladochealth.com

Teladoc Health is the global virtual care leader, helping millions of people resolve their healthcare needs with confidence. Together with our clients and partners, we are continually modernizing the healthcare experience and making high-quality healthcare a reality for more people and organizations around the world.