User Story: Service API for Provider Demographic Data View with TIN Validation and Session Logging

Connecting User Interface to Accurate Healthcare Provider Demographics

# Overview

This user story describes the requirements and expected functionality for a Service API that connects a user interface (UI) to a backend provider demographic data repository. The API must enable authorized users to view healthcare provider demographic information, support validation logic for the provider’s Tax Identification Number (TIN), and ensure that every session is logged for compliance and auditability.

# Background & Business Need

Healthcare organizations maintain large and sensitive databases of provider demographic information, such as name, address, contact details, affiliations, and regulatory identifiers (such as TIN). For operational efficiency and regulatory compliance, it is critical that these data be accessible in an accurate, secure, and user-friendly manner. A Service API that exposes this data to a UI enables seamless integration with various internal and external healthcare applications.

A specific business requirement is to ensure that only valid provider TINs are accepted and processed. The TIN must be exactly 9 digits in length, in accordance with federal regulations. Additionally, the API must log all session activity for the purposes of security, auditing, and compliance monitoring.

# User Story

Title: Service API connects UI to backend for provider demographic data view, with TIN validation and session logging

As a healthcare application user (such as an admin, support staff, or compliance officer),

I want the Service API to provide a secure and reliable connection between the UI and the provider demographic backend, so that I can query and view accurate provider information as needed,

And I want the API to validate that the provider’s TIN is exactly 9 digits before processing requests,

And I want every user session through the API to be logged with sufficient detail for auditing and compliance.

# Acceptance Criteria

* API Connectivity: The API must provide endpoints that can be securely and reliably accessed by the UI for the purpose of retrieving provider demographic data.
* Data Accuracy: The demographic data delivered to the UI must match the information in the backend database.
* TIN Validation: The API must include logic that verifies the TIN parameter is exactly 9 numeric digits.
* Error Handling: If the TIN is not 9 digits or contains non-numeric characters, the API must return a clear, actionable error message.
* Session Logging: Every session initiated by the UI to the API must be logged, including details such as session start/end time, user identifier, actions performed, and outcome (success/failure).
* Security Compliance: The API must authenticate and authorize all requests before providing access to protected data.
* Auditability: Logs must be retained in a secure location and be accessible for compliance audits.
* Performance: The API should deliver responses within an acceptable timeframe (e.g., under 2 seconds for standard queries).
* Scalability: The API should support concurrent requests from multiple UI users without performance degradation.

# Functional Requirements

* API Endpoint(s): The API must expose RESTful endpoints for retrieving provider demographic data, with endpoints secured using OAuth2 or similar authentication protocols.
* Request Parameters: The API must accept search parameters such as provider name, NPI (National Provider Identifier), and TIN.
* TIN Logic: Upon receiving a request that includes a TIN, the API will:
* Trim any whitespace or formatting characters.
* Verify that the TIN consists exclusively of numeric digits.
* Confirm that the TIN has a length of exactly 9 digits.
* If the TIN validation fails, the API will return an HTTP 400 error with a descriptive message (e.g., "TIN must be exactly 9 numeric digits.").

Session Logging: When a UI initiates a session with the API, the API will:

Create a unique session identifier for the request lifecycle.

Log the user ID, session start time, IP address, and any data access or actions performed.

Log the session end time and status (success or failure of requested operation).

Store all session logs in a secure, tamper-proof system for audit purposes.

Data Security: Encrypt all data in transit and at rest. Ensure API endpoints are only accessible to authenticated and authorized clients.

Error Management: All errors, whether due to TIN validation or session issues, must be logged with sufficient context to allow tracing and troubleshooting.

Data Consistency: The API must ensure that data presented in the UI reflects the most recent and accurate information in the backend.

# Non-Functional Requirements

* Scalability: The API must handle high volumes of requests, supporting peak loads and future growth.
* Availability: The API should be available 99.9% of the time, with appropriate monitoring and alerting for downtime.
* Performance: All demographic data queries should complete within 2 seconds under normal operating conditions.
* Logging Retention: Session logs must be retained for a minimum of 7 years, in line with healthcare auditing standards.
* Compliance: The design and operation of the API must comply with all relevant healthcare data regulations (such as HIPAA in the US).

# User Journey Example