# Narrative

Alice is a revenue cycle analyst for the Memorial Health System. Her job is to improve the revenue cycle end to end through workflow, from patient registration, capture of care billable events, insurance claims, to accounts receivable collection. It includes problem investigation and resolution. To perform her job Alice is authorized to view the demographic and clinical records for patients. She is not authorized to make changes to the data.

Bob is a security analyst for the Memorial Health System. His job includes reviewing accumulated Security Audit data to assure that the security policies are correctly implemented in software and are enforced. As part of this job he is authorized to review individuals’ Security Audit access history and patterns, and to trigger investigations when anomalous activity is discovered.

Bob notices that Alice has been viewing a large number of cases from the Emergency and Urgent Care departments. Looking into her access history over the past year, he sees that the number of cases has more than tripled over the past 2 months. He advises his manager, Carl, who, in turn, advises Alice’s manager, Diane, that an investigation will be made.

Carl obtains the Data Provenance records associated with the patients who have been viewed by Alice. A large number of them are household accidents, in particular involving children. He reports this to Diane.

Diane retrieves the Data Provenance records for child injuries and correlates them with Alice’s activity reports. The number of cases that Alice has reviewed does not correlate with her activity.

Diane reports this to Carl. She also schedules a meeting with Alice and invites Carl to attend. During the meeting, Alice admits that she has been gathering information for her friend who is a product liability attorney, who has been seeking clients for lucrative toy liability cases. Diane then terminates Alice’s employment and Carl immediately removes Alice’s authorization to access the Memorial Health System computer network.

Because this is a reportable Event under HIPAA, Carl and Diane document it, using the provenance records, and refer it to the Memorial Health System compliance officer for appropriate follow-up.

**Alternative Scenario**

Diane retrieves the Data Provenance records for child injuries and correlates them with Alice’s activity reports. The number of cases that Alice has reviewed correlates with her activity to improve ICD-10 coding and collection of revenue from health insurance for accidental injuries. Many of them involve children, incidentally. Diane reports this to Carl, and the investigation is closed.

# Ecosystem Entities

* Actors:
* Alice: A health system employee who is granted read-only access to a wide range of patient demographic, insurance, and clinical data.
* Bob: A health system employee who is granted read-only access to security audit repository data.
* Carl: A health system manager who has read-only access to Security Audit repository data and Data Provenance repository data, as well as read/write access to security management processes and data.
* Diane: A health system manager who has read-only access to Data Provenance repository data.
* Data Resources:
* Patient claims and treatment data, containing records of clinical data and the related charges, the claims sent to payors, and accounts recievable.
* Security Audit repository, containing records of all actions that are mediated using computer and network security processes. It is accessed only by authorized security administrators.
* Data Provenance repository, containing W5 (who, what, when, where, how) records for data creation, use, and life-cycle events. It is accessed only by authorized management staff.

# Technical Preconditions

* Explicit health system security and privacy policies exist, are congruent to federal and state regulations, and are enforced by the computer network and systems. The actual policies and enforcement mechanisms are out of scope for this use case.
* Automated processes for computer and network security management exist, and all security-mediated events are audited.
* Automated processes for data provenance and use exist, separately from security audit.
* Alice, Bob, Carl, and Diane are able to sign-on to the computer network and are granted authorities for process and data access appropriate to their job responsibilities.
* User interfaces and a data vocabulary for querying the Security Audit and Data Provenance resources exist. The specific user interface and report specific design, as well as the data vocabularies, are out of scope for this use case.

# Party-to-Entity Mappings

*Data flow and UML diagrams go here*

# Use Case Steps

## Normal Revenue Cycle Analysis Workflow for Alice

Alice is signed-on to the health system computer network

1. Alice constructs a queries to access claims data and treatment details for a class of patients.
2. Alice investigates the query results, looking for anomalies that indicate patterns that should be repeated (good collection results), or patterns that should be improved (poor collection results).
3. Alice formulates recommendations, forwards them to management for action, and summarizes them in her activity report.

## Normal Security Audit Workflow for Bob

Bob is signed-on to the health system computer network.

1. Bob constructs queries to access security audit data, looking for security-mediated actions for a class of users.
2. Bob investigates the query results, looking for anomalies that indicate unexpected use of the health system data resources or security policy violations.
3. If Bob notices anomalies, he analyzes them and forwards any significant findings to management for investigation.

## Investigative Workflow

1. [trigger] Carl receives a security anomaly report from Bob.
2. Carl retrieves the associated security audit data to identify the sources of anomalies.
3. Carl retrieves the associated provenance data to determine “who, what, why, where, and how” the anomalous events occurred.
4. Carl contacts the appropriate management (Diane, in this use case) to request an explanation.
5. Diane correlates the data from Carl with the associate employee activity reports.
6. If the activities are not legitimate, per policies and historical patterns, Diane initiate corrective actions
7. If the activities are legitimate, she reports it to Carl to end the investigation.