Brewers Buddy Website

Team 3 – Software Architecture Document

*Prepared for:*

**Penn State University**

**World Campus**

**SWENG 500**

Version: **1.0**

Date: 08/12/2013

Geoffrey Blogref

Gregg Ideus

Jonathon Parise

Jon Pistorius

Steve Platz

|  |  |  |  |
| --- | --- | --- | --- |
| DOCUMENT CHANGE HISTORY | | | |
| VERSION | | CHANGE DESCRIPTION | |
| No. | Date | Section | Narrative (of items affected) |
| 1.0 | 08/12/2012 | All | Initial Release |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1. Document Roadmap 4](#_Toc327303969)

[1.1 Description of the Architecture Documentation 4](#_Toc327303970)

[1.2 How Stakeholders Can Use the Architecture Documentation 5](#_Toc327303971)

[2. System Overview 6](#_Toc327303972)

[2.1 Business Goals 7](#_Toc327303973)

[2.2 System Context 9](#_Toc327303974)

[2.3 Functions 11](#_Toc327303975)

[2.4 Quality Attribute Requirements 14](#_Toc327303976)

[2.5 Constraints 16](#_Toc327303977)

[2.6 Architectural Drivers 17](#_Toc327303978)

[3. View Template 19](#_Toc327303979)

[4. Views 19](#_Toc327303980)

[4.1 Component and Connector View 19](#_Toc327303981)

[4.1.1 Primary Presentation 19](#_Toc327303982)

[4.1.2 Element Catalog (Components) 21](#_Toc327303983)

[4.1.3 Elements Catalog (Connectors) 22](#_Toc327303984)

[4.1.4 Element Catalog (Behavior) 25](#_Toc327303985)

[4.1.5 Architecture Background 26](#_Toc327303986)

[4.1.5.1 Performance Analysis 28](#_Toc327303987)

[4.2 Deployment View 29](#_Toc327303988)

[4.2.1 Primary Presentation 29](#_Toc327303989)

[4.2.2 Element Catalog for Deployment View 29](#_Toc327303990)

[4.2.3 Architecture Background 31](#_Toc327303991)

[5. Mapping Between Views 31](#_Toc327303992)

[5.1 Mapping Between Component-and-Connector and Deployment Views 31](#_Toc327303993)

[6. Rationale 32](#_Toc327303994)

Figures

[Figure 1: Conceptual View of System 9](#_Toc327303995)

[Figure 2: HIS System Context Diagram 10](#_Toc327303996)

[Figure 3: HIS Use Case Diagram 12](#_Toc327303997)

[Figure 4: System Architecture Diagram and Key (1) 20](#_Toc327303998)

[Figure 5: Sequence Diagram – User Login and Application Use 25](#_Toc327303999)

[Figure 6: System Architecture Diagram and Key (2) 26](#_Toc327304000)

[Figure 7: Deployment Diagram 29](#_Toc327304001)

Tables

[Table 1: Business Goals & Engineering Objectives 8](#_Toc327304002)

[Table 2: Quality Attributes, Engineering Objectives, and Scenarios 15](#_Toc327304003)

[Table 3: HIS Constraints 17](#_Toc327304004)

[Table 4: Architectural Drivers 19](#_Toc327304005)

[Table 5: Components & Responsibilities 22](#_Toc327304006)

[Table 6: Connectors and Responsibilities 23](#_Toc327304007)

[Table 7: Performance Figures 29](#_Toc327304008)

[Table 8: Deployment View Elements and Descriptions 30](#_Toc327304009)

[Table 9: Views and Relations 32](#_Toc327304010)

# Document Roadmap

The document roadmap describes what is contained within this document. It also gives direction to any stakeholder in which sections are most important based on their role.

## Description of the Architecture Documentation

This Brewers Buddy Website System Architecture Document contains the following sections:

**Section 1**

*Document Roadmap:*

An outline for the Architecture Documentation, it describes what the reader should expect to see within the document, as well as suggestions for which sections apply to a particular reader.

**Section 2**

*System Overview:*

This section lists the business goals and engineering objectives for the Brewers Buddy Website. This section also contains the context in which the system shall run a brief listing of functional requirements, quality attributes, and constraints. After reading this section, the reader will have a better understanding of what the Brewers Buddy Website architecture has set out to accomplish.

**Section 3**

*Architectural View Template:*

Provides a standard layout for the views presented in Section 4. After reading this section, the reader will know what to expect in the views described in the following section.

**Section 4**

*Software Architecture View:*

This section presents a view of the Brewers Buddy Website architecture that addresses the business goals outlined in Section 2. After reading this section, the reader will have a complete overview of the architecture chosen for the Brewers Buddy Website.

**Section 5**

*Mapping Between Views:*

Illustrates the differences and similarities between views and how they correlate to one another.

**Section 6**

*Rationale:*

Explanation and reasoning behind the architecture laid out in the preceding sections. After reading this section, the reader will understand why this architecture was designed in the way it was.

## How Stakeholders Can Use the Architecture Documentation

It is suggested that each stakeholder read Section 2. The System Overview section describes the goals the business wishes to accomplish, along with how those goals will be met by the System Architect. Following is a list of stakeholders and the sections they would deem most important.

*Someone new to the project*:

* Section 1: Architecture Document Roadmap
  + Once the roadmap has been read, decide for yourself which sections are most important.
* Section 3: Architectural View Template
  + This section provides an understanding for the data depicted in the views of Section 4.

*Project Manager:*

* Section 4.1: Component and Connector View
  + This section will identify integration points between different systems.
* Section 4.2: Deployment View
  + This section describes how each system will run within the existing, or new hardware.

*Software Architect:*

* Section 2.4: Architectural Drivers
  + This section identifies the most important features of the Brewers Buddy Website and their priorities.
* Section 4.1: Component and Connector View
  + This section will give a broad overview of how the architecture chosen for the Brewers Buddy Website looks and behaves.
* Section 6: Rationale
  + This section gives a detailed analysis of why certain choices were made and the reasoning for how the architecture was designed.

*Security Engineer:*

* Section 4.1: Component and Connector View
  + This section describes all of the systems within the Brewers Buddy Website architecture. The security engineer should focus on the security systems and how they protect the data.

*System Engineer:*

* Section 4.1: Component and Connector View
  + This section describes all of the systems within the Brewers Buddy Website architecture. The system engineer should focus on the integration points between all of the systems.

*Developer:*

* Section 2.3: Functions
  + This section outlines the tasks all of the actors expect to occur along with the functional responsibilities.
* Section 2.5: Constraints
  + This section describes the constraints of the architecture, which may give the developer clues as to what tools they are required to use.
* Section 4.1: Component and Connector View
  + This section describes all of the systems within the Brewers Buddy Website architecture. The developer should focus on the element catalog.

*Customer:*

* Section 2.1: Business Goals
  + This section describes the high level features and how the architecture meets them.
* Section 4.1: Component and Connector View
  + This section describes how the Brewers Buddy Website works and outlines the different systems it includes.

*User:*

* Section 4.1: Component and Connector View
  + This section describes how the Brewers Buddy Website works. It will give the user a fairly detailed look at just what the system can do. The User should pay the most attention to the element catalog, which includes a high level description of what each system does.

# System Overview

The Brewers Buddy Website was designed to help home brewers keep track of their home brews from start to finish. Home brewers need a place to keep their recipes, batches, and inventory numbers safe. They also would like to experiment from other batches created by other users as well as share their own. Brewers also wanted a unified software solution that could unite all home brewers in the street, neighborhood, city, or further. Finally, home brewers wanted a place where they could keep all their documents and not worry about losing them or destroying them.

The system described in the following sections seeks to meet, and exceed, the expectations that home brewers are wanting, and provide a solution, to those home brewers, that surpass their previous way of keeping track of their home brews.

## Business Goals

The business goals provided by the Integrated Health Network (IHN) providers are as follows:

* Build and maintain customer confidence by ensuring the security and privacy of all customer information.
  + By keeping security and privacy in mind during all levels of the design process, we hope to build a system that the IHN and its customers can feel confident using and trusting with their most personal health information.
* Provide patients anytime access to personal healthcare records
  + Allowing the patients of the IHN to access their own health information on their own terms is a major feature that will keep patients coming back to IHN providers.
* Create a single billing system to reduce billing errors and decrease administrative costs.
  + A single bill will improve the customer experience by showing a single face to all providers within the network of providers.
* Scale to support new markets and increasing patient base.
  + Entering new markets and increasing its patient base is important for any healthcare network to grow and remain competitive.
* Facilitate communication between medical professionals and patients.
  + Patients want a more personal relationship with their healthcare providers. This will also keep patients coming back to IHN providers.

Table 1: Business Goals & Engineering Objectives

|  |  |
| --- | --- |
| **Business Goal** | **Engineering Objective** |
| Build and maintain customer confidence by ensuring the security and privacy of all customer information. | Comply with laws and regulations governing the storage, processing and access to medical records. |
| Track all changes made to user data so an audit trail can be provided in the event of a breach or complaint. |
| Highly secure access to patient information from any location with specialized access controls based on user roles or attributes. |
| Enable the secure transmission and receipt of patient information by using proven security methods, protocols, and standards. |
| Support for remotely locking and wiping data from devices, owned by IHN providers that can access patient information. |
| Provide patients anytime access to personal healthcare records. | Support many different types of platforms and devices. |
| Recover gracefully from system faults to minimize downtime. |
| Remote, real-time access to patient information on-demand with minimal latency. |
| Create a single billing system to reduce billing errors and decrease administrative costs. | Provide single electronic billing system to be used across the IHN. |
| Ensure that bills are easy to understand to prevent customer confusion and service calls. |
| Scale to support new markets and increasing patient base. | Comply with all state and federal regulations for health care information. |
| Support for international languages. |
| Flexible infrastructure built to scale as the IHN grows. |
| Facilitate communication between medical professionals and patients. | Provide support for most major web-enabled devices (desktops, laptops, smart phones, tablets, etc.) |
| Provide electronic alerts and updates from providers to patients. |

## System Context

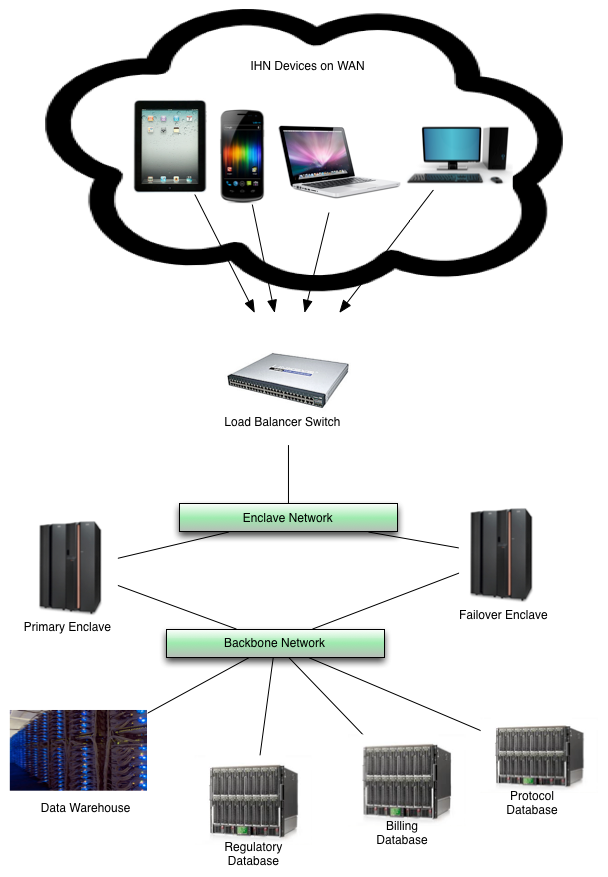


Figure 1: Conceptual View of System

The HIS system’s overall goal is to centralize health care data and make it easily accessible to patients, providers and IHN members. This health care data is stored in several databases and is accessible from many platforms over the network. Using various devices(computers, tablets smartphones) , users can view bill and update bills, access HIPPA regulations and other health protocols.

System availability is a high priority, health care information always needs to be accessible. To achieve this, a failover enclave is used. This failover will be automatically switched to if the primary system fails or is overburdened. The overall context of the HIS system is shown in figure 2 below.

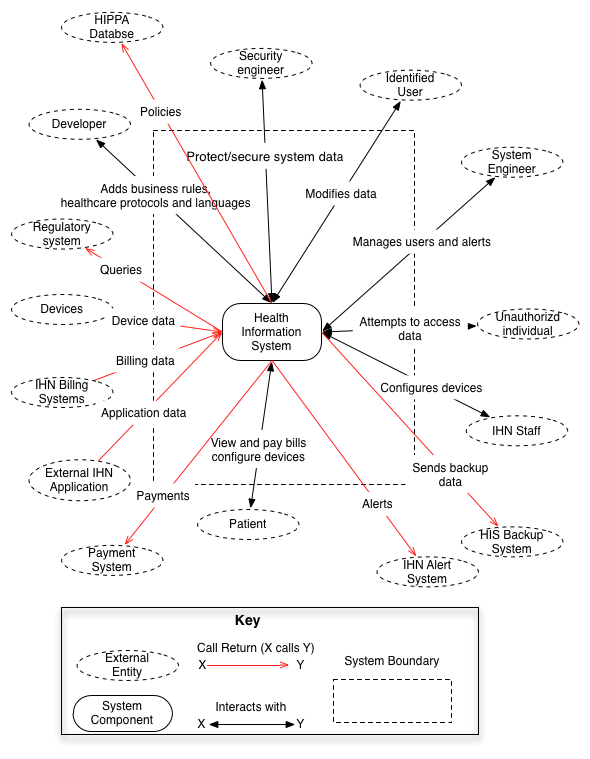


Figure 2: HIS System Context Diagram

In the context diagram above, the various users and systems that the HIS interacts with are shown. All of these interactions make up the functionality of the HIS system. This functionality is explained in detail in section 2.3.

## Functions

Figure 3 depicts a set of use cases that the Health Information System will allow all actors involved with the system to do. Some of these actions include adding new features, such as languages or health protocols. Adding a new language will help the system be more user friendly for both IHN providers and patients. When new health protocols are introduced, it will allow the system to remain compliant. Many functions in the diagram below also relate to a bill and how users interact with it. Providers will bill for services, which flows to a centralized system. That centralized system will combine all services for a given patient into one bill and send it to the patient.

Once the patient renders payment, the centralized system will process it and distribute funds to the appropriate IHN providers. In addition to the above features, security is a main focus. The data entered into the system must remain secure, so the patients can trust, not only the system, but the providers in which they do business with. All of these functions, and more, help the Health Information System to meet the Engineering Objectives laid out in Section 2.1.

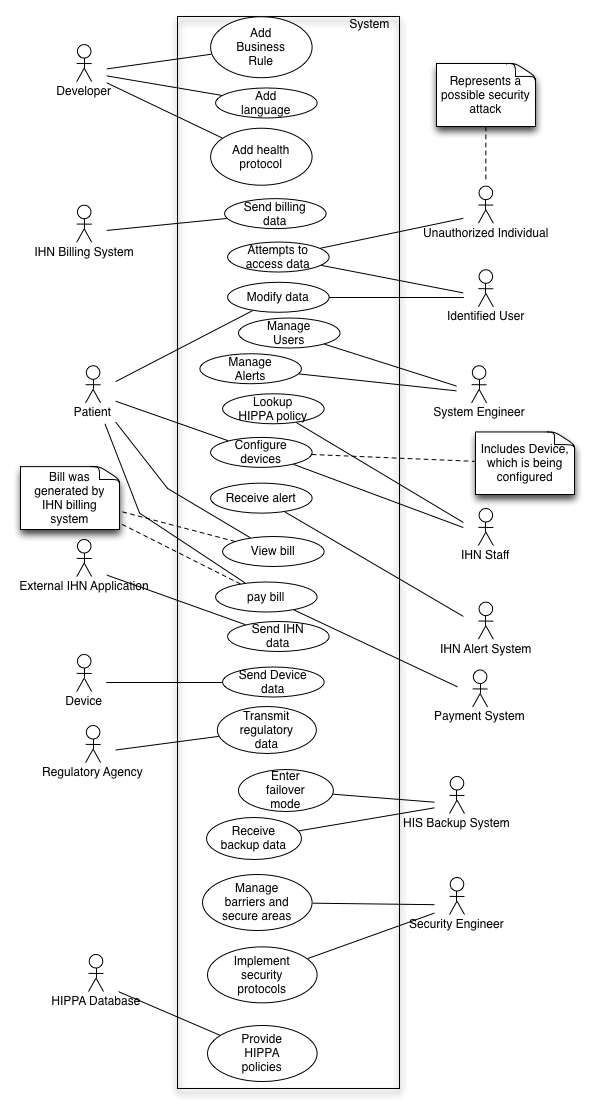


Figure 3: HIS Use Case Diagram

The following functional responsibilities can be derived from Figure 2:

1. Add, update and remove business rules without reinstalling the system.
2. Add, update and remove languages without reinstalling the system.
3. Add, update and remove health protocols.
4. Receive billing data from other IHN systems.
5. Generate a single bill from billing data from various IHN systems.
6. Maintain electronic billing records
7. Enable electronic bill pay through secure interface
8. Authenticate users to determine if they may access system data.
9. Authorize users to determine what they may access.
10. Block access attempts from unauthorized or unauthenticated users.
11. Allow only authorized users to modify data.
12. Prevent users from modifying data they are not allowed to modify.
13. Manage users and their access privileges.
14. Add, update, remove and configure devices.
15. Send alerts using an external alert systems
16. Translate system events into alerts.
17. Allow patients to view their single bills
18. Allow patients to pay bills.
19. Receive data from external IHN systems
20. Send and receive data from various devices.
21. Securely store all patient data.
22. Perform hot restart in the event of system failure
23. Maintain an audit trail of all changes to system data.
24. Remotely lock and wipe devices in the event of loss.
25. Distribute payment funds to IHN providers.
26. Ensure data confidentiality through encryption
27. Secure messages/data transmissions and protect integrity using proper protocols
28. Maintain firewalls, proxies, and secure enclaves to protect data
29. Regularly backup system data
30. Transmit communications between IHN members
31. Store patient records centrally for quick retrieval and/or updates
32. By using an open architecture, facilitate integration of disparate partner systems or components
33. Store and persist personalization content, such as user preferences.

## Quality Attribute Requirements

In Table 2 below, the Engineering Objectives are displayed, along with what type of quality it depicts. A specific scenario is also given which outlines an actor, a stimulus, an artifact, an environment, a response, and a response measure.

Table 2: Quality Attributes, Engineering Objectives, and Scenarios

| **Quality Attribute** | **Engineering Objective** | **Quality Attribute Scenario** |
| --- | --- | --- |
| Modifiability | Comply with laws and regulations governing the storage, processing and access to medical records | A developer is able to add a new business rule to the system at design time, the change will take less than 10 hours to make and test and no side effect changes will occur in the behavior. |
| Security | Track all changes made to user data so an audit trail can be provided in the event of a breach or complaint. | A correctly identified user tries to change data within the system while the system is connected. The system records the modifications by identity with a 99% probability of identifying the individual responsible for the modification. |
| Modifiability | Highly secure access to patient information from any location with specialized access controls based on user roles or attributes | A security engineer adds a new user role to the system at run-time, which is deployed with no negative impact to other roles or attributes. |
| Modifiability | Enable the secure transmission and receipt of patient information by using proven security methods, protocols, and standards | Security engineer implements open standard protocols at design time to ensure safe transport of system messages and non-repudiation while maintaining message integrity |
| Security | Support for remotely locking and wiping data from devices, owned by IHN providers, that can access patient information | An unauthorized individual attempts to access data on a device owned by IHN providers that is lost or stolen while it is connected. The device blocks access and wipes all data after 5 failed attempts with a 99% success rate. |
| Modifiability | Support many different types of platforms and devices | An IHN provider technical staff member is able to setup a device at runtime and is able to access patient information within 30 minutes. |
| Availability | Recover gracefully from system faults to minimize downtime. | An internal system crash occurs in a process during normal operation. The process logs the error and informs the operator of the problem. Only this single process is affected and the operator is able to correct the problem and continue using the system without downtime, no other operators are affected. |
| Performance | Remote, real-time access to patient information on-demand with minimal latency | Users initiate 2,000 transactions per minute stochastically under normal operations; these transactions are processed with an average latency of 3 seconds |
| Interoperability | Provide single electronic billing system to be used across the IHN | All billing information is sent to a centralized system to be processed where disparate bills will be combined. The centralized system will take no longer than 30 minutes to process and combine bills and will run once every 4 hours. |
| Usability | Ensure that bills are easy to understand to prevent customer confusion and service calls. | A user wants to comfortably understand their bill at run time. The system provides display system state that explains the bill with a user satisfaction rate of 75%. |
| Modifiability | Comply with all state and federal regulations for health care information. | A developer is able to add a new health care protocol to the system at design time, the change will take less than 10 hours to make and test and no side effect changes will occur in the behavior. |
| Modifiability | Support for international languages. | A developer is able to add support for a new language to the system at design time, the change will take less than 100 hours to implement and test and the change will not impact any other part of the system. |
| Modifiability | Flexible infrastructure built to scale as the IHN grows | Infrastructure engineer integrates new application into IHN infrastructure at design time within 6 hours with no impact to existing applications. |
| Usability | Provide support for most major web-enabled devices desktops, laptops, smart phones, tablets, etc.) | A patient wants to configure a device to view their medical records at run time. The system provides customizability options for this configuration. The patient completes configuration successfully within 5 minutes. |
| Modifiability | Provide electronic alerts and updates from providers to patients | A system administrator adds a new alert to the system at run-time and deploys the modification within 30 minutes with no impact to system operation. |

## Constraints

Table 3 (below) lists factors and descriptions of constraints on the Health Information System. The table outlines specific technologies, standards, or other things that affect how the architecture must be designed and developed.

Table 3: HIS Constraints

| **Category** | **Factor** | **Description** |
| --- | --- | --- |
| Organization | Healthcare Regulations | Healthcare regulations differ by state and how they’re executed can differ by location. HIS must adhere to these federal/state/local healthcare mandates and regulations at all times. |
| Organization | Patient Records | Patient data should only be viewed by the appropriate medical professionals and staff. Consent is required for access. |
| Product | Portability | HIS must be light-weight and usable on nearly and web-enabled computer or device at any time. |
| Product | User Network | A secure, easily navigable user network is necessary for providers to contact other providers and patients. |
| Product | Usability | An easy-to-use, customizable interface must be provided to users, especially for those who have particular impairment or disabilities. System must support various patient demographics and abilities such as age, disabilities, technological experience, etc. |
| Product | Security | System must be highly secure to protect user data. 99.9% of all system attacks must be stopped. |
| Product | Target Market | Limited by existing technical environment and/or skill set of technical staff. |
| Product | Security Standards | System must comply with latest security standards in the industry. |
| Product | Web Integration | To accommodate many devices, the front end, used by the end users and IHN staff members, will be built using a web rendering language (ASP.NET, PHP, Ruby, …) |
| Technology | Robustness and Responsiveness | HIS must be capable of processing multiple transactions simultaneously from multiple HIS-enabled devices. |
| Technology | Performance | HIS must consist of multiple distributed servers and be able to determine when a server or application is overloaded with users, and then siphon users or transactions to other servers as needed. |
| Technology | Openness and Flexibility | HIS must support most external systems that wish to integrate and share data. The architecture must be open to support different data formats and standards. |
| Technology | Scalability and Modernization | HIS must be built capable of supporting new technologies and capabilities to be “plugged into” the infrastructure in the future. |
| Technology | Message Security | HIS must secure all outgoing data and ensure the integrity of all incoming data for successful receipt or transmission. |
| Technology | Access Control Hierarchy | Users must be allocated to specific roles or attributes within the system to limit them only to functionality that they need. |
| Technology | Audit | HIS must log and store all system transactions to be reviewed by internal or external organization upon healthcare audits or reviews, |
| Technology | Continuity of Operations | Hot restart at a failover site must be provided to minimize system downtime in the event of failure or crash. |

## Architectural Drivers

Table 4 (below) contains a listing of the architectural drivers for the Health Information System. This table is in order of the highest to lowest priorities. Both the business and architecture team prioritized this list. The business’ priority is listed first in the priority column and is based on the following criteria:

* H - High; This is a major driving feature. If the system does not contain this feature, it will not be usable.
* M - Medium; This is a feature that will make this system stand out from a competitors comparable products.
* L - Low; This feature is not necessary for the system to have; although, time willing, it would be nice to include this feature.

The architecture team is listed second in the priority column of Table 4 and is based on the following criteria:

* H - High; This feature is a low level feature, or touches almost every system within the architecture; it would be hard to add this feature in once the design phase has completed.
* M - Medium; This feature impacts a whole system, or multiple systems within the architecture; these features could be changed once development has started without too much impact to the schedule.
* L - Low; This feature only impacts a portion of a system within the architecture, or only a piece of it; these features can be changed mid way through the development phase without much impact to the schedule.

Table 4: Architectural Drivers

| **No.** | **Architectural Driver** | **Priority** |
| --- | --- | --- |
| 1 | Enhanced security and auditing | (H, H) |
| 2 | Comply with new and changing health care laws. | (H, H) |
| 3 | Support for different user types requiring varying levels of access | (H, H) |
| 4 | Interoperate with existing and future IHN systems | (H, H) |
| 5 | Electronic creation, conversion, and storage of patient medical and billing data | (H, H) |
| 6 | Optimize load conditions for peak load/demand | (H, H) |
| 7 | System scalability to grow as the IHN grows. | (H, M) |
| 8 | Patient data storage and quick retrieval from a central location | (H, M) |
| 9 | Generate a single bill to patient | (H, M) |
| 10 | Retrieve patient medical info from anywhere | (H, L) |
| 11 | Backup system available on hot restart | (H, L) |
| 12 | Use recognized standards and protocols to facilitate COTS integration/upgrade | (M, H) |
| 13 | Facilitate communication via HIS | (M, H) |
| 14 | Latency of sending and receiving data. | (M, H) |
| 15 | Ease of user-to-user communications | (M, M) |
| 16 | Process all bills through a centralized system | (M, M) |
| 17 | Ability to add new languages. | (M, M) |
| 18 | Customizable alerts for system events | (M, L) |
| 19 | System personalization per user | (L, M) |
| 20 | Change data transmission protocols to support various devices | (L, M) |

# View Template

View is primarily focused on demonstrating the structure of component (element catalog) and its connectors. View further demonstrates the responsibility of each connectors in details along with the behavioral pattern among the components.

* Primary Presentation: displays the relationship between the elements and demonstrate the structure of the elements.
* Element Catalog: demonstrates in detail about all the component and their responsibility shown in the presentation in addition to elements expected behavior during runtime

Architecture Background: elaborates the design rationale and further demonstrates analysis results.

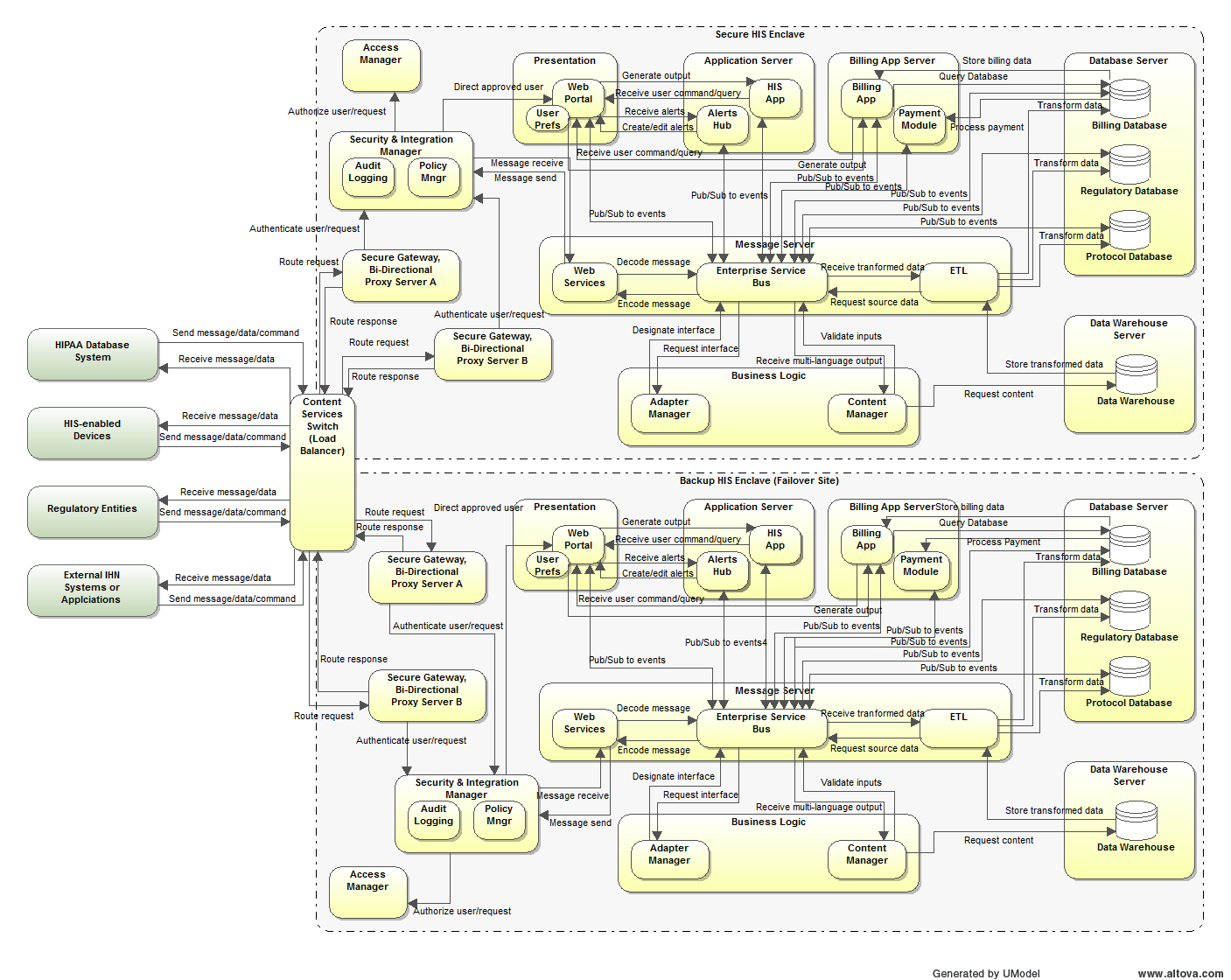
# Views

This section captures the different architectural and component views. Please see each individual section for further details.

## Component and Connector View

### Primary Presentation

The primary presentation is provided below. Each of the components are explained in further detail in Section 4.1.5.



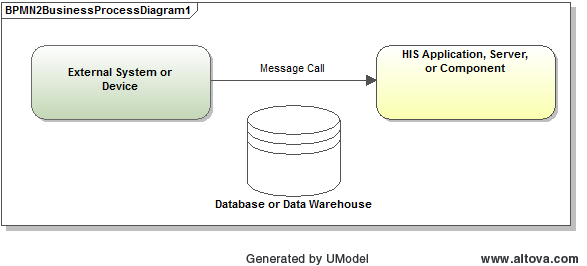


Figure 4: System Architecture Diagram and Key (1)

### Element Catalog (Components)

Table 5: Components & Responsibilities

| **Component** | **Responsibility** |
| --- | --- |
| Content Services Switch | * Manages all inbound connections from systems, devices, and others ensuring network availability, providing traffic management, load balancing, decreasing latency, and providing the first layer of security * Manages outbound data through a single point and filters to the appropriate recipient |
| Secure Gateway/Bi-Directional Proxy Server | * Monitors traffic in both directions ensuring the integrity and confidentiality of a message or transaction * Provides a firewall at entry to the HIS-secured enclave stopping any hostile connection or messages before they get any further |
| Security and Integration Manager | * Provides authentication services (proxy, implicit, explicit) and a policy decision service * Incorporates Web Service Security for message-level protection * Provides digital signature signing and other verification capabilities * Protects against various SOAP/XML payload attacks and intrusions * Provides audit logging for all transactions and messages |
| Access Manager | * Provides authorization services by maintaining the Access Control Lists and user roles |
| Presentation | * Provides a web-based interface for viewing the HIS Web Portal, managing alerts, accessing applications such as the billing application, and viewing backend data such as bills and medical records |
| Application Server | * Houses many HIS applications and functions such as the Alerts Hub, which provides all user and systems alerts * Provides space for other HIS applications and services |
| Billing Application Server | * Houses the HIS Billing Application and Payment module, 2 major components of the HIS system, which provide all billing and payment capabilities |
| Message Server | * Houses the HIS Enterprise Service Bus that provides the interfacing and communication between both internal and external systems and application * Filters all system messages to their proper destination * Provides web services to both secure and translate messages * Provides Extract, Transform, and Load functionality to take disparate data, transform it into something useful for HIS, and send it to an end-point |
| Business Logic | * Provides an adapter manager to send and receive data in different formats such as FTP, SFTP, JMS, HTTP/S, etc. * Enables content management to ensure data is not duplicated unknowingly, simplify the storage and retrieval of data, provide translation functionality, make it easier for users to communicate, and facilitate with reports |
| Database Server | * Houses all system databases including Billing, Regulatory, and Protocol databases. These databases store all relevant information to their names |
| Data Warehouse Server | * Houses the HIS data warehouse which stores all HIS and partner system information in one central location and provides archival functions |

### Elements Catalog (Connectors)

Table 6: Connectors and Responsibilities

| **Component** | **Responsibility** |
| --- | --- |
| Publish / Subscribe | * Handles asynchronous events from HIS-enabled systems and devices and supports dynamic subscription to these events |
| Publish Events and Messages to Web Portal | * Publishes events and messages to the Web Portal that the Web Portal user or integrated system has subscribed to |
| Subscribe to Events and Messages from Web Portal | * Subscribe to events from end-users with HIS-enabled devices that the Web Portal user has subscribed to |
| Web Portal sends user commands to relevant HIS App | * User commands are input through the web-based interface and sent along to the relevant system or application. For example, the user clicks to initiate the Billing Application from the Web Portal. This will send the commands along to navigate the user to it |
| Application Generates Output to Web Portal | * Any of the hosted applications, such as the Billing Application, will create a response to a user command which is in turn displayed on the user’s web-based interface |
| Publish Events and Messages from Application (Alerts, Billing, etc.) | * Publishes events and messages from an application to the Web Portal for the end-user or integrated partner system |
| Subscribe to Events and Messages from Application (Alerts, Billing, etc.) | * Subscribe to events from end-users with HIS-enabled devices via the Web Portal user and messages from integrated partner systems outside of the Secure HIS Enclave |
| Application Routes Query to Database | * An application sends along a user or system query to the relevant database via the Web Portal or system message |
| Database Returns Query Result(s) | * The database processes the query and returns an appropriate response to the end-user or partner system |
| ETL System Transforms Internal or External Database Data | * The ETL system receives data from an internal or external database or source and transforms the data into a useful format for the HIS system. |
| Data Warehouse Stores Transformed Data | * The Data Warehouse accepts extracted, transformed, and loaded data into the data warehouse for storage and reference |
| ETL Requests Data for Transformation from ESB | * ETL actively searches for data to be transformed for a universal format for the HIS system from the ESB |
| ESB Forwards Messages and Data to be Transformed for Storage | * The ESB forwards along any flagged messages or data to the ETL system for transformation and subsequent use or storage |
| Web Services Encode Outgoing Messages | * The ESB prepares messages for transit from HIS to external partner systems or end-users. Web services then encode the message through the message header before it can be sent out |
| Web Services Decode Incoming Messages | * When a message is received and it has passed through security, before it can be interpreted it must be decoded using the same web services that encoded it. This ensures the message integrity and non-repudiation. |
| ESB forwards requests for multi-lingual support to Content Manager | * The content manager receives any translation requests piped through the ESB and makes changes according to the available libraries. This can manifest in terms of a translated Web Portal page, for example |
| Content Manager Validates Data | * Before data is sent for storage or to a system or application, it can be flagged for validation first before and changes are made. The Content Manager requests data to be sent to it, which it will then check to ensure there are no discrepancies, redundancies, or other errors. |
| ESB Requests Adapter Interface from Adapter Manager to Send/Receive Message | * When a message interface is setup between HIS and a partner system, a messaging interface is setup, sometimes more than one. This can be FTP, SFTP, HTTP/S, etc. When receiving or sending a message to/from these partners, the ESB will need to request the interface is in place to perform these actions. |
| Adapter Manager Designates and Confirms Interface for ESB | * The Adapter Manager receives the request to confirm interface setup for messaging. The Adapter Manager confirms the setup is in place and that messages can be sent/received accordingly. |
| Patient, System, or Entity Requests Access to HIS | * This connection is implied through sending/receiving messages and events to HIS |
| Patient, System, or Entity Sends Message, Data, or Command | * The patient, system, or entity performs an operation through the presentation layer which is directed by the application or ESB. Or the system or entity sends a message from itself to HIS which must clear security and be received and processed. |
| Patient, System, or Entity Receives Message, Data, or Command | * The patient, system, or entity received a response to their command or message. This can be in the form of a visible action at the presentation layer or message sent out from HIS to the intended recipient. |
| Content Services Switch Routes Request to Secure Gateway | * When a message or command is sent to the system from an outside entity, it must first be routed to a more available authentication server before passing through further security. |
| Secure Gateway Routes Response to Content Services Switch | * When a message is being sent out, it must be routed back out through the Content Services Switch to be routed to the proper recipient. |
| Secure Gateway Performs Authentication Using Security and Integration Manager | * The Secure Gateway Refers to the Security and Integration Manager for authentication by proxy, the majority of authentication requests. This ensures a patient, system, or other entity is allowed to access the system. Implicit and explicit authentication will be performed by the Security and Integration Manager, itself. |
| Security and Integration Manager Uses the Access Manager to Perform Authorization | * The Security and Integration Manager will refer to the Access Control Lists and other features stored in the Access Manager to proper route the user or message once they have gained access to the HIS system and provision them with the correct privileges as assigned. |
| Security and Integration Manager Directs User to Presentation Layer | * Once a user has been authenticated and authorized, they are forwarded to the secure Web Portal at the Presentation Layer to begin using the HIS system and its applications. |
| Content Services Switch Directs Patients, Systems, and Entities to Failover Site | * It is implied in the diagram, but if the primary HIS Enclave has a system failure or any particular component has a failure, the Content Services Switch directs these individuals, systems, and entities to the failover site where they can use these system and applications without even noticing that the ones at the primary site are down. |

### Element Catalog (Behavior)

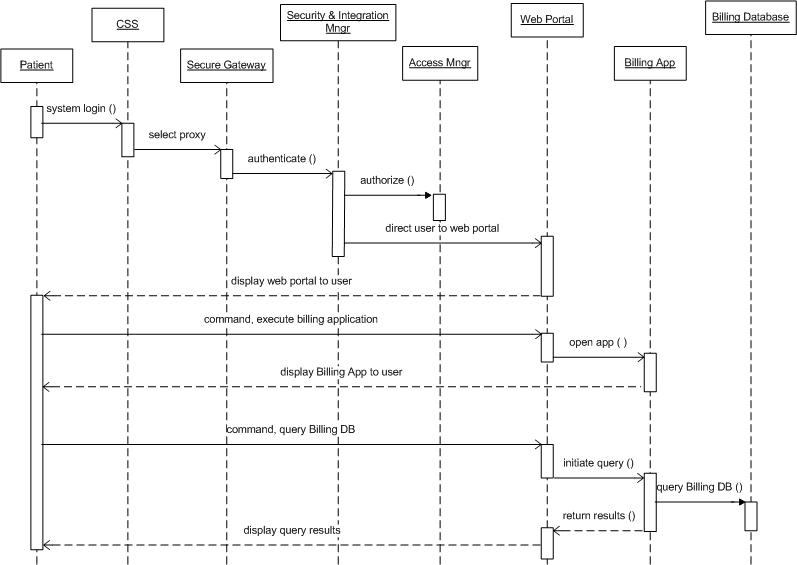
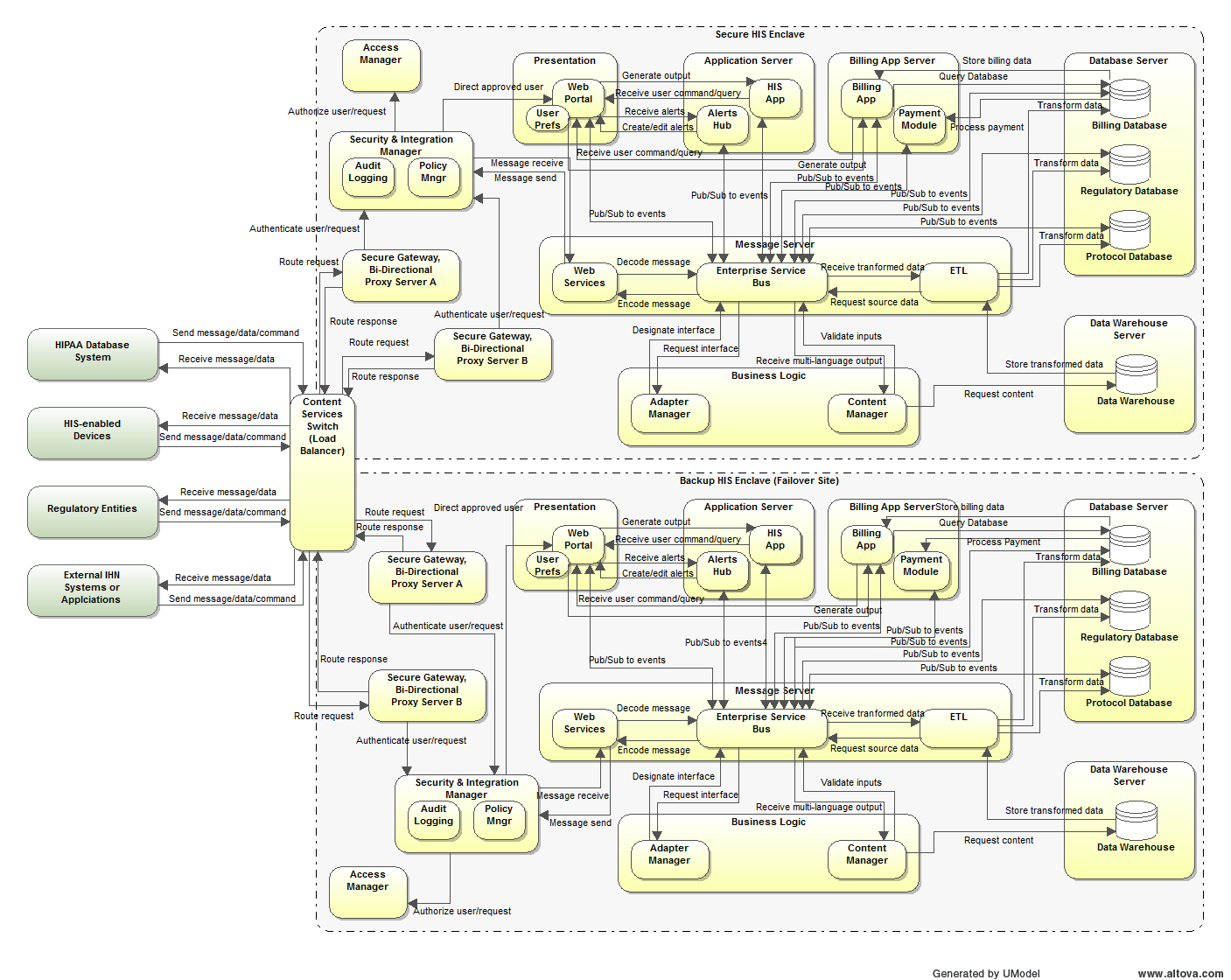


Figure 5: Sequence Diagram – User Login and Application Use

The above sequence diagram captures login from a patient or system user and subsequent system use. The patient or user logs in and is authenticated and authorized by the Secure Gateway/Security and Integration Manager and Access Manager, respectively. Once they have cleared the security checkpoints, the patient or user is directed to the Web Portal where they have access to HIS applications and data.

A patient or user then is able to access the application, in this case the Billing Application, by issuing a command to the Web Portal interface. In this particular instance, the patient or user is querying the database. The system passes this query along from the application to the database. The database then responds with any applicable results which are in turn displayed in the Web Portal.

### Architecture Background



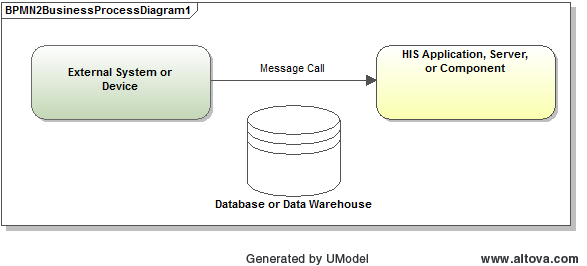


Figure 6: System Architecture Diagram and Key (2)

The components and features depicted in the architecture diagram above include the following items which provide the accompanying benefits:

* Content Services Switch
  + Ensures high availability
  + Provides an initial layer of security
  + Reduces of latency
  + Provides load balancing capabilities
* Secure Gateway, Bi-Directional Proxy Servers A & B
  + Provides a firewall to fend off attacks
  + Enables the safe transit of messages to and from HIS
* Security & Integration Manager
  + Contains an intrusion detection system (IDS) to catch unwanted users
  + Performs implicit and explicit authentication and authentication by proxy
  + Provides Web Services Security and ensures message integrity and confidentiality.
  + Maintains an audit trail and policy decision service
* Access Manager
  + Enables the safe management of user access
  + Contains lists of user roles
* Presentation
  + Displays Web Portal and applications
  + Visualizes communications and alerts
* Application Server
  + Houses the majority of small to mid-sized HIS applications.
  + Enables the transit of messages and data to and from the hosted applications
* Billing Application Server
  + Houses the Billing Application and Payment module
  + Enables the transit of messages and data to and from the hosted applications
* Database Server
  + Houses each of the HIS databases
  + Maintains billing/payment, regulatory, and protocol information among other materials
  + Enables the transit of messages and data to and from the hosted databases
* Data Warehouse Server
  + Houses the centralized HIS Data Warehouse
  + Maintains all HIS data for storage and reference
  + Enables the transit of messages and data to and from the hosted databases
* Message Server
  + Houses the Enterprise Service Bus (ESB), which routes all messages both internally and external to HIS
  + Provides message security and translation services
  + Enables the transformation of data through ETL
* Business Logic
  + Enables the use of different adapters to send and receive system messages
  + Provides content management services to better manage data and provide dictionary translations of material
* Failover Site
  + Exists in the event of catastrophic failure of HIS or hosted applications
  + Regularly backed up so data loss is minimized

#### Performance Analysis

The table below shows the performance analysis for each step required for a user to view their bill, as shown in the sequence diagram in section 4.1.4. This is a three part action, with the user issuing three commands. The first command is a login command, the second is a open app command (launch the app) the third is a query bill(view bill) command.

In the table below, the work units indicate how difficult the computations for the step are on a 1-5 scale, with 5 being the most difficult. The messages column indicates how many system messages are sent to complete the step.

Table 7: Performance Figures

|  |  |  |
| --- | --- | --- |
| **Processing Step** | **Work Unit** | **Network Messages** |
| System Login | 1 | 6 |
| OpenApp | 2 | 3 |
| Query billing | 4 | 5 |

The system login step does not require much processing, it simply needs to verify the user’s login information. Regardless of whether the login is successful or not, the number of messages will be 6, because in both cases a screen is shown to the user.

The open app step is a bit more complex, it requires the application to be loaded and the various possible options to be calculated and displayed. This step requires 3 messages to handle the user command and provide a response.

The query billing step is the most complex. It requires a query to be run against the database to generate the users bill for display. Depending on how many records are present for the user, this could get quite complex. There are 5 messages required for this step, this includes issuing the command, running the query and displaying the results.

## Deployment View

### Primary Presentation

The following diagram indicates the physical location of the HIS services and software components. Each of the components is depicted with a host server.

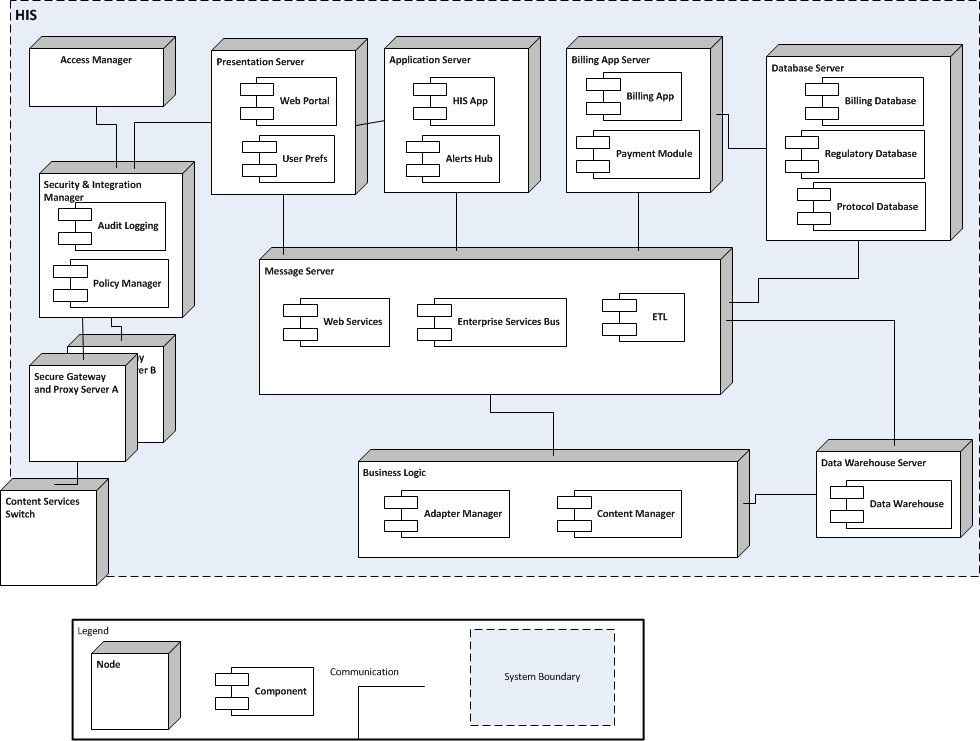


Figure 7: Deployment Diagram

### Element Catalog for Deployment View

Table 8: Deployment View Elements and Descriptions

|  |  |
| --- | --- |
| **Element** | **Description** |
| Access Manager | Maintains users access and list of roles |
| Audit Logging | Maintains records of all systems transactions |
| Policy Manager | User authentication |
| Secure Gateway and Proxy Servers A&B | Firewall to secure system boundary |
| Content Services Switch | Contains functionality to enable security enclave, and failover |
| Web Portal | Displays system user interface |
| User Preferences | Enables customization of the user experience |
| HIS App | Hosts the small and mid-sized applications |
| Alerts Hub | Generates System Alerts |
| Billing App | Hosts the Billing Application |
| Payment Module | Hosts the Payment Application |
| Billing Database | Contains the billing information for patients |
| Regulatory Database | Contains the regulations that govern the HIS |
| Protocol Database | Contains the protocols that guide the HIS |
| Web Services | Hosts the message security and translation services |
| Enterprise Services Bus | Prepares messages for transit from HIS to external partner systems or end-users |
| ETL | Transforms internal or external data for stoppage or display |
| Adapter Manager | Designates and confirms interface readiness for ESB |
| Content Manager | Validates data before storage or display |
| Data Warehouse | Contains the patient data for the HIS |

### Architecture Background

The deployment of the services was designed to satisfy or enhance the capabilities of the system to achieve the greatest number of architectural drivers. These include the following:

|  |  |  |
| --- | --- | --- |
| **No.** | **Architectural Driver** | **Priority** |
| 1 | Enhanced security and auditing | (H, H) |
| 6 | Optimize load conditions for peak load/demand | (H, H) |
| 8 | Patient data storage and quick retrieval from a central location | (H, H) |
| 11 | Backup system available on hot restart | (H, L) |
| 14 | Latency of sending and receiving data. | (M, H) |

# Mapping Between Views

Mapping between views draws comparisons between different views of the system highlighting areas that are common to these views.

## Mapping Between Component-and-Connector and Deployment Views

Table 9: Views and Relations

| **C&C View** | **Deployment View** | **Relation** |
| --- | --- | --- |
| Billing Database | Database Server | The named C&C elements are part of the deployed component |
| Regulatory Database |
| Protocol Database |
| Data Warehouse | Data Warehouse Server |
| Billing App | Billing App Server |
| Payment Module |
| HIS App | Application Server |
| Alerts Hub |
| Access Manager | Access Manager |
| Audit Logging | Security and Integration Manager |
| Policy Manager |
| Web Services | Message Server |
| Enterprise Service Bus |
| ETL |
| Secure Gateway, Bi-Directional Proxy Server A/B | Secure Gateway and Proxy Server A/B |
| Adapter Manager | Business Logic |
| Content Management |
| Web Portal | Presentation Server |
| User Preferences |
| Content Services Switch | Content Services Switch |

# Rationale

*Business Context*: As the Integrated HealthCare Network (IHN) expands and offers its services to a broader community spanning multiple time zones, it is necessary to have a centralized system that can sustain growth and support new market areas. Due to the growing number of health care facilities, hospitals, physicians, etc. a centralized access to patient medical records is important to provide prompt services. In addition to that there is a need to increase efficiency and productivity of IHN related facilities and physician. As the laws pertaining to industry and privacy policies including privacy and security change continuously, IHN is required to streamline its processes for compliance.

To sustain this growth and above mentioned demands, IHN has decided to develop a Health Information System (HIS). HIS will help IHN to scale and provide services to organizations associated to IHN and to the community it serves. IHN would achieve larger market share with the new platform and can adapt to policy changes frequently resulting in new revenues stream.

*Key Features*:

* Centralized information: Provide patients anytime access to personal healthcare records and consolidated single bill.
* Increase Accessibility and efficiency: Accommodate various field devices and communication among medical professionals.
* Enhanced security and access control.
* New market share: Scale to support new market share with compliance to regulations and support new languages.