Group Assignment 1.1: A Conceptual Model of Architecture

Jacob Harrison

Joshua A Wortz

Stephanie Wright

University of San Diego

Course Number: CSOL-520

Melanie Thomas, M.S.

03/03/2025

Problem Statement

This proposal outlines the development of a scalable and secure software architecture for Bene Gesserit Urgent Care Offices' (BGUC) integrated urgent care management system. The system will encompass electronic medical records (EMR), online check-in, prescription transmission, insurance processing, payment processing, and seamless data synchronization across multiple locations. The scope includes designing and implementing a centralized data platform, user interfaces for patients and healthcare providers, secure APIs for interoperability with pharmacies, insurance providers, and primary care networks, and a PCI-compliant payment system. System boundaries will be clearly defined to prevent unauthorized access, ensuring compliance with HIPAA and PCI-DSS standards. Deliverables will include a functional prototype, system documentation, security frameworks, and a deployment roadmap.

Key limitations include dependency on external systems, such as pharmacy networks, insurance providers, and payment processors, which may introduce latency and integration challenges. Constraints will involve regulatory compliance with HIPAA and PCI-DSS, data privacy mandates, and resource availability for implementation. Assumptions include reliable internet connectivity, adherence to industry-standard security protocols, and stakeholder willingness to adopt new workflows. Potential failure points include data synchronization issues between locations, security vulnerabilities in third-party integrations, and scalability bottlenecks if the system is not optimized correctly. Payment processing risks such as transaction failures, compliance gaps, or security breaches could also impact financial operations and patient trust. Addressing these risks through robust architectural planning and continuous security assessments will be critical to project success.

Entity Class Descriptions

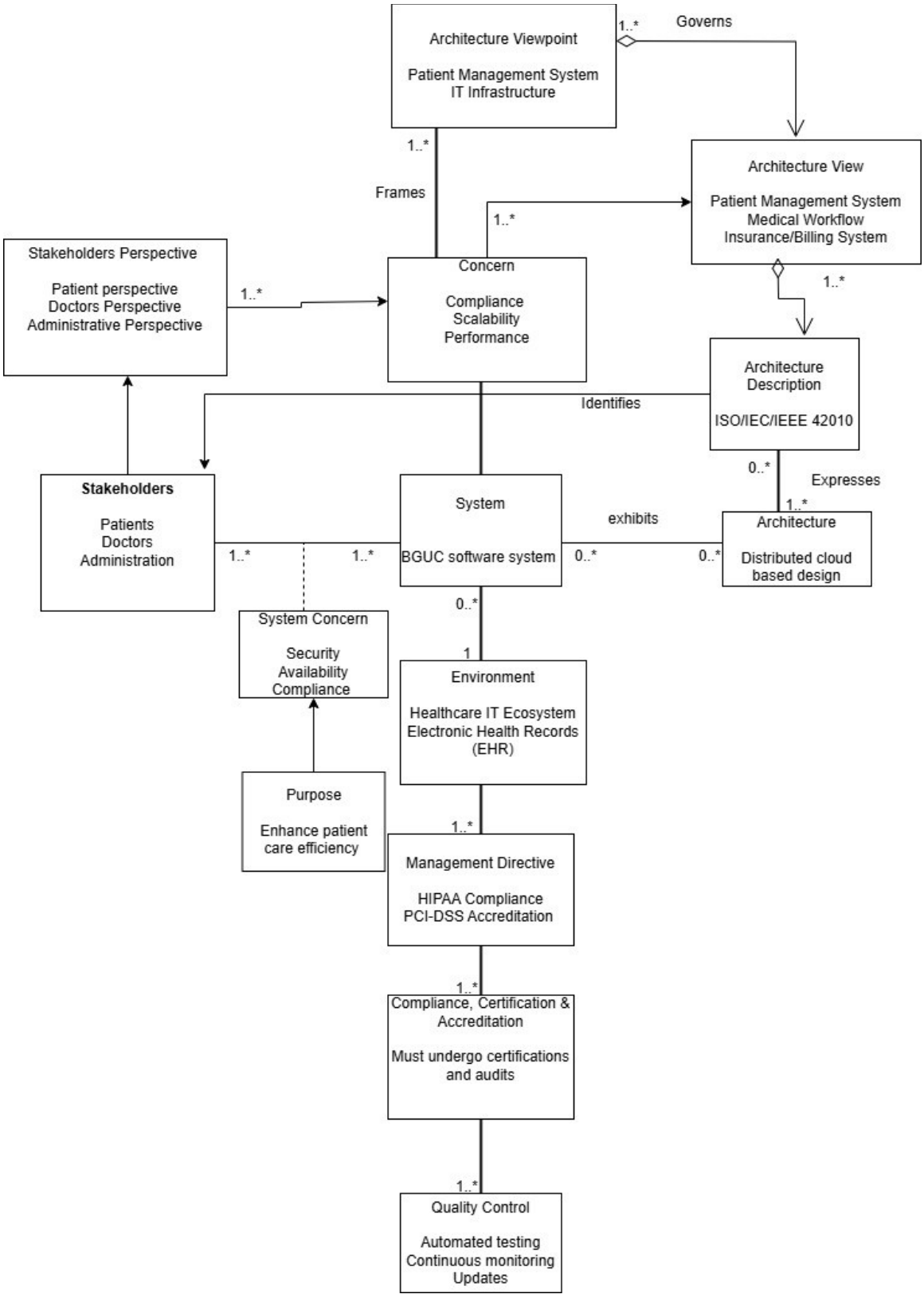
1. **System**—The BGUC software system consists of an integrated urgent care management platform that enables patient check-in, medical record management, electronic prescription processing, insurance claims handling, and PCI-compliant payment processing. The system is designed to comply with **HIPAA** and the **HITECH Act**, ensuring the secure handling of electronic health records (Alder, 2025).
2. **Stakeholders** – Key stakeholders include **patients** (end-users requiring medical services), **doctors and medical staff** (who interact with patient records and prescriptions), **administrators** (responsible for operational oversight), **IT and security teams** (who maintain system integrity and compliance), **insurance providers** (who process claims), **pharmacy networks** (that receive electronic prescriptions), and **payment processors** (that handle financial transactions). Stakeholders also include cybersecurity entities that help mitigate **ransomware risks**, as highlighted by CISA (n.d..).
3. **Environment** – The system operates in a **healthcare IT ecosystem**, including electronic health records (EHR), third-party insurance and pharmacy networks, regulatory frameworks (HIPAA, PCI-DSS), and cloud-based infrastructure, enabling secure data sharing across BGUC locations. The **Health Industry Cybersecurity (HIC) framework** emphasizes the importance of cyber hazard information sharing for secure data exchange in healthcare (Healthcare and Public Health Sector Coordinating Council, 2023).
4. **System Concern** – Primary concerns include **security** (protecting patient data from ransomware and breaches), **availability** (ensuring system uptime for urgent care

needs), **compliance** (meeting HIPAA, HITECH, and PCI-DSS standards), **interoperability** (seamless integration with third-party services), and **scalability** (supporting new locations and increasing patient demand). Implementing NIST's **attribute-based access control (ABAC)** model can enhance security by ensuring role-based access to sensitive patient data (National Institute of Standards and Technology [NIST], 2014).

5. **Purpose** – The primary purpose of the BGUC system is to **enhance patient care efficiency** by streamlining check-ins, medical record access, prescription fulfillment, insurance claims, and payment processing. This digital transformation aligns with the **HITECH Act's** goal of promoting electronic health records to improve care quality and efficiency (Alder, 2025).
6. **Architecture Description**—The **ISO/IEC/IEEE 42010** standard defines architecture description as a structured approach to documenting system components, interactions, and constraints (International Organization for Standardization, International Electrotechnical Commission, and Institute of Electrical and Electronics Engineers, 2011). BGUC's architecture description will include **security, interoperability, and regulatory compliance models**, ensuring alignment with operational goals and industry standards.
7. **Architecture** – The BGUC system architecture follows **a distributed cloud-based design**, incorporating **secure patient portals, provider interfaces, administrative dashboards, and encrypted APIs for interoperability**. It also features **redundant infrastructure** to ensure system resilience and prevent service disruptions, which is critical for healthcare operations (NIST, 2022).
8. **Management Directive**—BGUC's executive leadership issues policies and strategic goals, such as ensuring **HIPAA and PCI-DSS compliance**, maintaining service availability, and investing in **secure and scalable infrastructure**. Management

directives will be guided by **NIST's cybersecurity resource guide** for HIPAA security rule implementation (NIST, 2022).

9. **Compliance Certification & Accreditation** – The system must undergo rigorous certification and audits to meet industry standards, including **HIPAA compliance** for patient data protection, **PCI-DSS accreditation** for secure payment transactions, and **interoperability certifications** for data exchange with pharmacies and insurance providers. Regular audits and **security assessments** help ensure continuous compliance (Healthcare and Public Health Sector Coordinating Council, 2023).
10. **Quality Control** – Quality control measures include **automated testing** (for functionality and security), **continuous monitoring** (for system health and performance), **incident response plans** (to address security threats), and **user feedback mechanisms** (to refine usability and workflow efficiency). Following **CISA's ransomware protection strategies** will help reduce cybersecurity threats (CISA, n.d..).


Architecture Viewpoint
Patient Management System
IT Infrastructure
1..*
Governs
1..*
Frames
Architecture View
Patient Management System
Medical Workflow
Insurance/Billing System
1..*
Stakeholders Perspective
Patient perspective
Doctors Perspective
Administrative Perspective
1..*
Concern
Compliance
Scalability
Performance
1..*
Architecture Description
ISO/IEC/IEEE 42010
Identifies
0..*
Expresses
1..*
Stakeholders
Patients
Doctors
Administration
1..*
1..*
System
BGUC software system
exhibits
0..*
0..*
Architecture
Distributed cloud based design
System Concern
Security
Availability
Compliance
0..*
1
Environment
Healthcare IT Ecosystem
Electronic Health Records (EHR)
Purpose
Enhance patient care efficiency
1..*
Management Directive
HIPAA Compliance
PCI-DSS Accreditation
1..*
Compliance, Certification & Accreditation
Must undergo certifications and audits
1..*
Quality Control
Automated testing
Continuous monitoring
Updates

References

Alder, S. (2025). What is the HITECH Act? *HIPAA Journal.* https://www.hipaajournal.com/what-is-the-hitech-act/

Cybersecurity and Infrastructure Security Agency. (n.d.). How can I protect against ransomware? *U.S. Department of Homeland Security.* Retrieved February 26, 2025, from https://www.cisa.gov/stopransomware/how-can-i-protect-against-ransomware

Healthcare and Public Health Sector Coordinating Council. (2023). *Health industry cybersecurity—Cyber hazard information sharing.* https://healthsectorcouncil.org/wp-content/uploads/2023/07/HIC-CHIRP-FINAL_1.pdf

International Organization for Standardization, International Electrotechnical Commission, & Institute of Electrical and Electronics Engineers. (2011). *ISO/IEC/IEEE 42010:2011—Systems and software engineering—Architecture description.* https://cdn.standards.iteh.ai/samples/50508/ec3d9367f48e4b28a7ac8dddaeca5a3f/ISO-IEC-IEEE-42010-2011.pdf

National Institute of Standards and Technology. (2022). *Implementing the health insurance portability and accountability act (HIPAA) security rule: A cybersecurity resource guide (Initial public draft, NIST Special Publication 800-66r2)*. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.ipd.pdf

National Institute of Standards and Technology. (2014). *Guide to attribute-based access control (ABAC) definition and considerations (NIST Special Publication 800-162).* U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf