Group Assignment 2.1: Defining Goals and Objectives

Jacob Harrison

Joshua A Wortz

Stephanie Wright

University of San Diego

Course Number: CSOL-520

Melanie Thomas, M.S.

03/10/2025

Enterprise Goals and Objectives

Bene Gesserit Urgent Care aims to maintain a prominent level of urgent care performance that enhances our patients' experience, protects their sensitive data, and ensures compliance with the Healthcare Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI-DSS). BGUC prioritizes the integration of EHR (electronic health records) with pharmacies and insurance providers while maintaining uninterrupted, readily available, and secure data interoperability. The goal is to create a platform that makes healthcare services seamless for healthcare administrators and increases the quality of healthcare services for patients.

Organizational Success Factors:

BGUC’s success depends on complying with regulation standards, maintaining a secure cloud architecture, and establishing strong cybersecurity practices. BGUC’s compliance with HIPPA ensures that patients' health records are being secured, while compliance with PCI-DSS secures financial transactions for patients and third-party affiliates. Implementing cloud-based services guarantees the scalability and elasticity of our infrastructure, allowing for secure remote access capabilities for healthcare providers. Consequently, BGUC’s affiliated third-party networks, including insurance providers and pharmacies, operate within a system that supports interoperability functions, thereby minimizing disruptions to essential healthcare services.

Technology Goals (High Level):

BGUC's infrastructure will be developed on a cloud-based architecture, providing dependable, secure, and scalable services to ensure both availability and efficiency. All BGUC systems will adhere to the CIA triad (confidentiality, integrity, availability), ensuring employees recognize the significance of safeguarding patients' classified data following HIPAA standards and protecting financial transactions to cooperate with PCI-DSS standards. The employment of secured APIs will produce effective communication between healthcare providers, third-party affiliates, and EHR systems. Systems will be secured through encryption protocols to protect patient information and ensure system redundancies do not disrupt operations, maintaining consistent availability. BGUC aims to employ technology that facilitates real-time data integration across multiple locations, ensuring the seamless daily functioning of critical healthcare operations.

Technology Factors:

The use of various technologies that support BGUC functions will play a crucial role in its infrastructure. Encryption guarantees compliance with HIPPA standards, which protect all confidential data transmissions. Implementing secure APIs to ensure secure communication between BGUC and its supply chain vendors will deter unauthorized access. Due to the implementation of cloud computing standards, BGUC's systems will be scalable and consistently available. Automated data backups will be used to prevent data loss and ensure the activation of disaster recovery protocols when necessary.

Security Goals:

BGUC’s priority regarding security is to protect private patient data, prohibit unauthorized access, and decrease cybersecurity threats to healthcare systems. BGUC prioritizes compliance with HIPPA and PCI-DSS regulations to protect patient healthcare records and ensure the security of patient financial transactions. The implementation of Role-Based Access Controls (RBAC) will be necessary to restrict access to records containing sensitive information, ensuring that only authorized personnel can modify or update any patient records. Deploying continuous security monitoring applications and conducting regular risk assessments are essential for identifying and addressing vulnerabilities in critical infrastructure. This approach enables BGUC to deter security incidents proactively.

Security Success Factors:

Several key security factors must be implemented to achieve BGUC's security goals. Multi-factor authentication (MFA) will be needed to address unauthorized intrusions into healthcare systems. Network firewalls and intrusion detection software will be required to monitor and restrict threat actors from accessing the secured network. Installing regularly scheduled penetration testing and security auditing is necessary to ensure system resiliency from cybersecurity threats. BGUC’s incident response plan will be comprehensive to minimize disruptions to daily operations and effectively address security incidents.

Policies

BGUC is dedicated to delivering top-quality care when it is needed most, with extended hours to accommodate urgent medical needs. This includes evenings, weekends, and holidays, ensuring patients have access to care beyond typical office hours. Some locations may even operate 24/7 to provide comprehensive coverage for urgent health concerns.

Additionally, BGUC has built strong partnerships with local primary care providers, ensuring smooth coordination between urgent care and ongoing healthcare. When patients visit BGUC, their medical records are promptly updated and shared with their primary care provider, maintaining seamless continuity of care.

Procedures

BGUC provides an online check-in system to simplify the process and reduce wait times. Patients can fill out required forms and check in online before their visit, minimizing time spent in the waiting room. BGUC also collaborates with a broad range of insurance providers, including PPOs, HMOs, Medicaid, and Medicare, ensuring that patients from various insurance plans can access care without significant obstacles.

Standards

BGUC is committed to delivering medical treatments, procedures, and diagnostic services that meet the highest patient safety standards. This includes precise

diagnoses, evidence-based treatment protocols, and clear patient communication. BGUC employs board-certified physicians, nurse practitioners, and other qualified healthcare professionals with the necessary licenses and credentials. All clinical staff must maintain their certifications and participate in continuous education to stay current with the latest medical advancements and best practices.

Guidance

At BGUC, align with the mission of providing accessible, high-quality urgent care while staying committed to innovation and patient satisfaction. To ensure this, the mission should be regularly reviewed and updated to reflect emerging healthcare trends and new technologies.

As BGUC expands to new locations, maintaining consistent service quality across all facilities must remain a top priority. Standardized procedures should be implemented while allowing flexibility to address each community's unique needs.

Investing in leadership development programs is key to equipping staff with the necessary skills to manage patient care effectively, optimize operations, and promote teamwork. Additionally, BGUC should offer continuous educational opportunities for employees to stay informed about evolving healthcare practices and technological advancements.

Risk Appetite

Given the importance of patient safety and health outcomes, BGUC would likely adopt a low to moderate risk appetite for clinical care. The organization must remain committed to providing high-quality medical care by adhering to strict clinical protocols and safety standards. While BGUC may accept operational risks, such as integrating new technologies or experimental treatments, these decisions would only be made after thorough evaluation, training, and pilot testing to ensure their safety and efficacy.

To mitigate these risks, BGUC would prioritize evidence-based practices, regular staff training, and strict adherence to medical standards and regulations, reducing the likelihood of patients. With rapid advancements in healthcare technology, BGUC may adopt a moderate to high-risk appetite when embracing new technology and innovations that can enhance patient care, operational efficiency, and service delivery. (Risks, 2023).

Compliance Requirements

BGUC must adhere to HIPAA regulations, which govern the confidentiality, privacy, and security of patients' health information. This requires BGUC to ensure that patient medical records and personal health information (PHI) are protected and disclosed only with patient consent or as required by law, in line with the Privacy Rule. Additionally, with the Security Rule, BGUC must implement security measures to protect electronic PHI (ePHI) against threats like unauthorized access or cyberattacks. If a data breach occurs, BGUC will notify affected individuals and report the breach to the

Department of Health and Human Services (HHS) within a specific time frame, following the Breach Notification Rule.

In addition to federal regulations, BGUC must also comply with state-specific healthcare regulations, which may vary by state. These typically include ensuring that all medical providers are licensed where they practice, adhering to the state's defined scope of practice for healthcare providers, such as nurse practitioners, physician assistants, and physicians. If BGUC is classified as a hospital-based emergency care provider, it must comply with the Emergency Medical Treatment and Labor Act (EMTALA). This involves providing appropriate screening and stabilizing treatment to all individuals, regardless of their ability to pay (Alder, 2023).

References

Alder, Steve. (2023). *HIPAA Compliance and Urgent Care.* https://www.hipaajournal.com/hipaa-compliance-and-urgent-care/

Risks, U. (2023, October 18). *Managing Risks in Urgent Care Settings*. Retrieved from U.S. Risks: https://prep.usrisk.com/insights/10-18-23-managing-risks-in-urgent-care-settings/.