*For instructions on using this template, please see Notes to Author/Template Instructions on page 11.*

**Healthy Body Wellness Center (HBWC)**

# High-Level Technical Design

**Version X.X**

**Table of Contents**

[High-Level Technical Design 1](#_Toc525646265)

[1. Introduction *(Not required for performance assessment)* 4](#_Toc525646266)

[2. Current Systems 4](#_Toc525646267)

[3. Goals, Objectives, and Rationale for New or Significantly Modified System 4](#_Toc525646269)

[3.1 Project Purpose 4](#_Toc525646270)

[3.2 System Goals and Objectives 4](#_Toc525646271)

[3.3 Proposed System 4](#_Toc525646272)

[3.3.1 System Scope 4](#_Toc525646273)

[3.3.2 Processes Supported 4](#_Toc525646274)

[3.3.3 High-Level Functional Requirements 4](#_Toc525646275)

[3.3.4 Summary of Changes 5](#_Toc525646276)

[4. Factors Influencing Technical Design 5](#_Toc525646278)

[4.1 Relevant Standards 5](#_Toc525646279)

[4.2 Assumptions and Dependencies 5](#_Toc525646280)

[4.3 Constraints 5](#_Toc525646281)

[4.4 Design Goals 5](#_Toc525646282)

[5. Proposed System 5](#_Toc525646284)

[5.1 High-Level Operational Requirements and Characteristics 5](#_Toc525646285)

[5.1.1 User Community Description 6](#_Toc525646286)

[5.1.2 Nonfunctional Requirements 6](#_Toc525646287)

[5.2 High-Level Architecture 6](#_Toc525646288)

[5.2.1 Application Architecture 7](#_Toc525646289)

[5.2.2 Information Architecture 8](#_Toc525646290)

[5.2.3 Interface Architecture (*not required for performance assessment)* 8](#_Toc525646291)

[5.2.4 Technology Architecture 8](#_Toc525646292)

[5.2.4.1 Platform 9](#_Toc525646293)

[5.2.4.2 System Hosting 9](#_Toc525646294)

[5.2.4.3 Connectivity Requirements 9](#_Toc525646295)

[5.2.4.4 Modes of Operation 9](#_Toc525646296)

[5.2.5 Security and Privacy Architecture 9](#_Toc525646297)

[5.2.5.1 Authentication 9](#_Toc525646298)

[5.2.5.2 Authorization 9](#_Toc525646299)

[5.2.5.3 Encryption 9](#_Toc525646300)

[6. Analysis of the Proposed System 10](#_Toc525646301)

[6.1 Risks 10](#_Toc525646302)

## Introduction

*Not required for performance assessment.*

## Current Systems

HBWC primary business process is designed around providing hospitals grants to conduct health research. This process is initiated with the National Institute of Health issuing funds to HBWC for Health research grants. This triggers the Office of Grants Giveaway to begins their work in assigning funds to hospitals in the form of grants. Information pertaining to grants, the hospitals receiving the grants, and the subsequent research conducted are all entered and managed in the COTS application SHGTS. This COTS application is currently running on Access 2010 which does not support concurrent users. Funding for grants that are awarded to hospitals are transferred using an ACH and logged in the SHGTS application. Executive staff of the OGG the only individuals authorized to distribute grant funds based on grant evaluations that are entered in the SHGTS application by OGG principal investigators. These funds are delivered to the hospitals in the form of paper checks that are logged in QuickBooks and SHGTS application. Remote offices and users’ access SHGTS application over patient information and research data are kept in Excel spreadsheet and stored on HBWC secured file server prior to its entry into the SHGTS database as an evaluation. This information remains the property of the Principal Investigator for 1 year at which point, the data becomes the property of the NIH. Hard copies of all reports are made and stored in a secured file cabinet. This process is not sustainable with the NIH adhering to the Paper Reduction Act by moving the application process to an online form.

HBWC employee on\offboarding and Payroll process is completely manual. New hire applicants are required to complete a paper application which is available only in the Human Resources office or upon request, can be mailed to the applicant via US Postal Service. These applications are manually reviewed and processed by HR personnel for use by department heads within the organization. Once a candidate has been selected, HR mails an offer letter with a return envelope for acceptance. Upon receipt of the acceptance of the offer, HR then begins the process of Onboarding the new hire. This process can take up to 21 days after receiving responses to a position posting. Time is collected on paper sheets, manually entered in QuickBooks, stored for historical purposes in file cabinets in a climate-controlled room with other Organizational Financial records. QuickBooks is used to generate bi-weekly paychecks for each of the employees in the company.

## Goals, Objectives, and Rationale for New or Significantly Modified System

### Project Purpose

The purpose of this project is to address HBWC’s desire to migrate to a cloud based HRMS while continuing to fulfill its mission “to help patients take responsibility for their overall wellbeing and educate members of the local community in the practice of wellness.” Once completed, HBWC have received sufficient modifications to its infrastructure to accommodate the new HRMS, with security being addressed throughout development and implementation of the project.

### System Goals and Objectives

* Modernize its payroll and benefits management processes
  + Implement ADP SaaS to manage HR, Payroll, and Benefit processes.
  + Implement Direct Deposit Services for Payroll
* Redesign the SHGTS database to improve its efficiency, availability and security
  + Migrate SHGTS database to Azure SQL Server HA 2 node Cluster
  + Implement RBAC to secure access to data and available database views.
* Construct public, partner, and internal secured web portals
  + Build Azure DevOps to manage development of Web portals
* Properly categorize and label all HBWC information data points
  + Utilize Microsoft 365 Compliance to Label and Protect sensitive data

### Proposed System

* Redesign HBWC Infrastructure network topology to SD-WAN which will allow the support of increased traffic, user base, and remote sites.
* A proper PKI Infrastructure will be established to allow the issuance and maintenance of user and device certificates.
* ADP SaaS solution will be integrated into HBWC business processes to manage Payroll and Benefits.
* Migrate QuickBooks SaaS and integrate with ADP SaaS
* Develop Web application to modernize the SHGTS database utilizing Azure PaaS Services
* Enhance physical and logical security of HBWC assets using Azure Identity Services, Milestone X-protect Professional and Comm-Core Door security systems.

#### System Scope

System scope includes the following:

* Migrate HR and Payroll to SaaS Cloud
* Implement DevOps in PaaS Cloud
* Reinforce Logical and Physical Infrastructure Security initiatives to accommodate the move to the cloud.
* Implement SD-WAN Network to remote sites
* Disaster recovery site to support ADP and Azure services

#### Processes Supported

The processes that the proposed solution will support are as follows:

* User, system, and service authentication with multi-factor authentication enforced on users and One Time Passwords for service accounts.
* Role based Access Controls will be enabled to secure systems, applications, access to information and physical access to sensitive areas of the company.
* Single Sign-On will be implemented to allow seamless authentication and authorization of users to various web based and installed applications
* Cloud based HR Benefits management, Payroll Services and HR Automation will be supported through ADP SaaS.
* Disaster Recovery Site will be used to support critical systems if HQ is not available.
* Azure DevOps will be used to support ongoing development of the new SHGTS web application, HBWC Intranet portal, HBWC Internet website, and other future development endeavors.
* HBWC infrastructure will support the increased network traffic, future expansions and acquisitions.
* HBWC new Hybrid Cloud infrastructure will accommodate dynamic capacity scaling to meet all changes in the demand placed on the infrastructure.

#### High-Level Functional Requirements

The following are the high-level functional requirements of this proposed solution:

* Purchase of ADP SaaS
* Purchase of Azure PaaS
* Compliance with NIH Security Requirements
* Purchase of additional WAN circuits for remote sites and circuit redundancy
* Implementation of Role-Based Authentication
* Purchase of Azure Cold Storage for archival purposes
* Purchase & Implementation of physical security throughout the organization.
* Purchase of space, equipment, software and licenses for new DR Site.

## Factors Influencing Technical Design

### Relevant Standards

The following standards will be taken into consideration during the design of this solution:

* ISO/IEC 27001 Information Security Management
  + This requirement provides the framework for building an effective Information Security Management System to secure financial, employee PII, Intellectual Property and Hospital Research data across multiple platforms, media and locations.
* HIPAA of 1996
  + Adhering to title 2, and 3 of the HIPAA statues is mandatory due to the interaction, transmittal and storage of Patient data pertinent to research performed by Hospitals that are awarded grants provided by the NIH.
* Sarbanes-Oxley Act of 2002
  + Multiple Titles under the SOX federal law will shape how and where financial data is stored as well as who has access to view or modify said data.
* IEEE 2675-2021 IEEE Standard for DEVOPS
  + This industry standard will be used to govern the creation of HBWC DevOps process to ensure the principles of DevOps are in place and that communications between stakeholders, developers and operations staff remains effective and reliable.
* NIH numerous security requirements

### Assumptions and Dependencies

The follow assumptions are made in the design of this solution:

* Downtime will be unavoidable, but will be mitigated to reduce impact to business
* The integrity of data is critical to the business and paramount during the migration of services and processes to the cloud.
* Training will be needed for users and administrators of the new systems.
* HBWC will retain responsibility of business continuity and disaster recovery during the migration
* This solution assumes that HBWC is currently in compliance with federal and local regulations

### Constraints

The following constraints have been placed on the design of this solution:

* Federal and Local regulations pertaining to health, personal Identifying, and financial data.
* Absolute requirement of maintaining CIA during the migration of data in transit and while at rest.
* Available budget
* Target date to complete the deployment of the solution.

### Design Goals

The design goals for this solution include the following:

* Dynamic Scalability of Cloud and Physical Infrastructure
* Improved logical and physical security
* Maintenance of compliance of industry standards and regulations
* Retirement of “End of Life” applications and hardware
* Streamlined processes and procedures throughout the organization
* Expansion of VPN capabilities to secure data in transit.

## Proposed System

### High-Level Operational Requirements and Characteristics

#### User Community Description

**Table 1: User Community Description**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **User Group** | **Description/Expected Use of System** | **Type**  **(Federal Employee, Contractor)** | **Geographic Location** | **Network Profile**  **(LAN, WAN, External)** | **Total Users** | **Concurrent Users** |
| *HBWC*  *Users* | *HBWC Employees with Non-Elevated Rights* | *Employee* | *Worldwide* | *LAN/WAN* | *300+* | *250+* |
| *Contractor* | *Outside temporary staff* | *Contractor* | *Worldwide* | *LAN/WAN*  *External* | *50+* | *25+* |
| *Partner* | *Hospital Staff, NIH Staff & other Partners requiring limited access* | *Federal/Business* | *Worldwide* | *External* | *20* | *15+* |
| *HBWC*  *ADMIN* | *HBWC Employees with Elevated Rights* | *Employee* | *HQ* | *LAN/WAN* | *6* | *6* |
| *HBWC Executives* | *HBWC/OGG Executive staff* | *Employee* | *HQ* | *LAN/WAN* | *6* | *6* |

#### Nonfunctional Requirements

|  |  |
| --- | --- |
| **ID** | **Requirements** |
| NFR.0001 | Employee training on use of new systems will be needed. |
| NFR.0002 | Policies and procedures will be needed for new business processes |
| NFR.0003 | SaaS and PaaS platforms will require elasticity to accommodate varying usage loads. |

### High-Level Architecture

Graphical user interface, application

Description automatically generated

Diagram

Description automatically generated

**Table 2: Alternatives Considered for the Overall Architecture**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Alternative** | **Description** | **Pros** | **Cons** | **Preferred Alternative?** | **Rationale** |
| *REDESIGN* | *Complete replacement of Infrastructure* | *Up to date technology* | *High Cost*  *Training* | *No* | *CBA too high* |
| *MODIFY EXISTING* | *Augment current technologies with Cloud Solutions while replacing EOD tech* | *Allows growth*  *Addresses deficiencies*  *Improved Performance* | *Increased Dev time*  *Moderate Costs* | *Yes* | *CBA provides good cost to benefit.* |
| *KEEP EXISTING* | *Leave Infrastructure in place and continue using* | *Low expenditure*  *No loss of time* | *Failure to comply with NIH Standards*  *Imminent system failure*  *Hard/Software not supported* | *NO* | *Does not meet HBWC goals* |

#### Application Architecture

**Table 3: Description of Application Components**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Application Component** | **Description**  **(Business Process Supported, Purpose of Component)** | **Type**  **(Identify both (1) Operational or Analytical and (2) Batch or Online)** | **Strategy**  **(Build, Buy, Reuse, Rewrite)** | **Alternatives** | **Pros** | **Cons** | **Preferred Alternative** |
| *SHGTS Azure Database* | *Grants Process* | *Operational*  *Online* | *Buy & Build* | *On-premise SQL Server* | *Meets needs for growth & Availability* | *Added Cost*  *Administrative overhead* | *Yes* |
| *SHGTS Web Portal* | *Grants Process* | *Operational*  *Online* | *Build* | *None* | *Provides interface to data using RBAC for limited views* | *Development time*  *Need for ongoing development* | *Yes* |
| *ADP SaaS* | *HR Payroll & Benefits* | *Operational & Analytical*  *Online* | *Buy* | *UKG Pro*  *Workday*  *PeopleSoft* | *Allows modernization of HR process* | *Requires end user and administrative training*  *Security of data in transit* | *Yes* |

#### Information Architecture

**Table 4: Description of Information Components**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Conceptual Information (Entity)** | **Description** | **Type of Data Store (Transactional or Analytical)** | **System of Record?** | **Data Acquisition Approach**  **(e.g., User Data Entry, Interface)** | **Alternatives** | **Pros** | **Cons** | **Preferred Alternative** |
| *Employee PII* | *PII related to employees Payroll and Benefits* | *Transactional* | *Yes* | *HR Staff & Employee data entry @ ADP web* | *Records store in File cabinets* | *Ease of access*  *Modernization of process* | *Increased security vulnerability footprint* | *Preferred* |
| *Research Data* | *Hospital Research Data* | *Analytical* | *Yes* | *Hospital data entry/ NIH data access @ web portal* | *Excel Spreadsheets stored on file server* | *Increased security of data*  *Quick storage and retrieval of data* | *Training on use of new web portal needed by staff* | *Preferred* |
| *Financial Data* | *HBWC grant and payroll data* | *Transactional and Analytical* | *Yes* | *HR Staff data entry* | *QuickBooks*  *Workforce*  *Peoplesoft* | *Speed of processing Payroll and Grant Funding* | *Recurring cost* | *Preferred* |

#### Interface Architecture

*Not required for performance assessment.*

#### Technology Architecture

Augmentation of existing architecture will be needed to meet the increased network traffic. Updated firewalls will be deployed at each branch to facilitate the implementation of SD-WAN and regional client VPN services. All outdated and end of life hardware will be replaced with hardware that will be under warranty and support. Each branch will be outfitted with two internet circuits for Fault Tolerant connections to HBWC HQ. Redundant connections to Azure and ADP will be established to HQ to ensure the availability of communications and transfer of information.

##### Platform

A hybrid cloud platform will be designed to support the ADP SaaS and Azure PaaS solutions. This platform will include on-premise Active Directory, FTP, and File servers as well as physical routers, switches, and security appliances. In the cloud, there will exist web applications, load balancers, virtual servers, and networks that will communicate with HQ on-premise network. Azure Identity and Access Management will work in conjunction with on-premise Active directory to secure all assets within HBWC Network leveraging RBAC.

##### System Hosting

HR Benefits and Payroll services will be hosted by SaaS provider ADP North America. DevOps, Identity Access Management, File and Database Services will be hosted by PaaS provider Microsoft Azure. WAN connectivity between sites will hosted by service providers local to the site.

##### Connectivity Requirements

Connectivity within HBWC will consists of Gigabit connections from IDF closets to individual desktops. Connections between IDF’s and to the MDF will be 10 Gigabit uplinks. Internet circuits will vary by site based on the capabilities of local ISP providers. Wireless AP’s will be strategically placed throughout each site. Each site will have a Wireless Controller in the MDF with a 10 Gigabit uplink to the core router. Each site will have an out-of-band cellular modem for that will be used as a tertiary connection that will become available if both circuits are no longer available.

##### Modes of Operation

Galois Counter Mode (GCM) will be the primary mode of operation as it combines encryption and authentication. This mode is designed to provide high throughput on high-speed data links with low latency and cost.

#### Security and Privacy Architecture

Defense in depth will be used provide layered security to ensure multiple levels of security to secure HBWC infrastructure and data. In addition to layered security, NIST Risk Management Framework will be implemented to ensure HBWC has the capabilities and process in the form of a risk management program to manage information security, privacy risk for the organization, and meet the requirements of Federal Information Security Modernization Act being required by the NIH.

##### Authentication

Authentication for basic users will make use of MFA, SSO, and RBAC which will be managed by Azure Identity Access Controls, Intune, on-premise Active Directory and Azure Active Directory.

Users with elevated access will use a 3rd Authentication factor requiring the use of a Token provisioned by on-premise FortiAuthenticator.

Access to research and PII data collected and used by the hospitals and the NIH will require an alternative 3rd authentication factor, a Common Access Smart Card. Each of these 3rd factor forms of authentication will integrate with SSO services to allow seamless access to various platforms withing HBWC.

##### Authorization

Role Based Access Controls managed by a combination of security groups and Azure Information Protection. All users and systems will have their respective levels of access controlled by groups assigned to the accessing party. Based on ACL’s applied to the groups assigned, the user will be granted or denied access. All access requests will be logged and correlated for auditing purposes.

##### Encryption

Asymmetric Encryption will be used for all secured communications and data transmittal outside HBWC. Symmetric Encryption will be used internally where needed. Some systems may have a need to use Hybrid Encryption to secure the data and the connection that it traverses. The following are a few of the known assets that will require encryption:

* File Encryption
* Disk Encryption
* Email Encryption
* VPN Encryption
  + Site to Site
  + End User

## Analysis of the Proposed System

### Risks

* Physical Access to HWBC facilities is not monitored or reported on.
  + Mitigated –Physical security of HBWC sites will be accomplished by use of Azure Identity Services, Milestone X-protect Professional Camera and Comm-Core Door security systems.
  + Reasoning – Ensuring the physical access to HBWC sites and subsequent asset is core to establishing Defense in Layers and greatly increases the C.I.A. triad.
* Lack of systems and applications patch management
  + Mitigated – Develop systems and application update process to incorporate OS, application, and Firmware.
  + Reasoning – Lack of patch management procedures will lead to increased attack surface of company, system failures, and could allow an intrusion to go undetected.
* Insufficient or lack of an Information Security System
  + Mitigated – Develop process, procedures, and regulations within HBWC that will address the confidentiality, Integrity, and Availability of its data, assets, and personnel.
  + Reasoning – Insuring INFOSEC is in place is required by NIH.
* There are no Cryptographic controls in place
  + Mitigated – Establish and enforce Cryptographic Controls policy that will address Confidentiality, Integrity, Authentication, and Non-repudiation of sensitive or critical information in HBWC.
  + Reasoning – Cryptographic controls policies will ensure uniformed use of encryption, Digital Certificates, and SSH keys.
* Log Correlation and retention not in place or practiced at HBWC
  + Mitigated – Established cloud-based syslog services. All server and infrastructure equipment securely relays logged information to service for correlation and reporting.
  + Reasoning – Implementation of syslog services reinforces Non-Repudiation of access and actions taken against HBWC assets and data.

*Instructions: Prioritize and describe the top* ***five*** *risks that the preferred alternative presents. For each risk, describe if it will be mitigated or accepted, and justify your decision.*

**Appendix A: Referenced Documents**

***(Optional: Not required for performance assessment)***

*Instructions: Summarize the relationship of this document to other relevant documents. Provide identifying information for all documents used to arrive at and/or referenced within this document (e.g., related and/or companion documents, prerequisite documents, relevant technical documentation, etc.).*

**Table 9: Referenced Documents**

|  |  |  |
| --- | --- | --- |
| **Document Name** | **Document Location and/or URL** | **Issuance Date** |
| *<Document Name>* | *<Document Location and/or URL>* | *<MM/DD/YYYY>* |
| *<Document Name>* | *<Document Location and/or URL>* | *<MM/DD/YYYY>* |
| *<Document Name>* | *<Document Location and/or URL>* | *<MM/DD/YYYY>* |

**Appendix B: Notes to the Author/Template Instructions**

*This document is a template for creating a high-level technical design for a given investment or project. The final document should be delivered in an electronically searchable format. The high-level technical design should stand on its own with all elements explained and acronyms spelled out for reader or reviewers.*

*This template includes instructions, boilerplate text, and fields. The developer should note that:*

* *Each section provides instructions or describes the intent, assumptions, and context for content included in that section. Instructional text appears in blue italicized font throughout this template.*
* *Instructional text in each section should be replaced with information specific to the particular investment.*
* *Some text and tables are provided as boilerplate examples of wording and formats that may be used or modified as appropriate.*

*When using this template, follow these steps:*

1. *Table captions and descriptions are to be placed left-aligned, above the table.*
2. *Modify any boilerplate text, as appropriate, to your specific investment.*
3. *Do not delete any headings. If the heading is not applicable to the investment, enter “Not Applicable” under the heading.*
4. *All documents must be compliant with Section 508 requirements.*
5. *Figure captions and descriptions are to be placed left-aligned, below the figure. All figures must have an associated tag providing appropriate alternative text for Section 508 compliance.*