Healthy Body Wellness Center

Case Study

**Healthy Body Wellness Center (HBWC) Mission and Vision**

The Healthy Body Wellness Center’s mission is to help patients take responsibility for their overall wellbeing and educate members of the local community in the practice of wellness. The HBWC includes an Office of Grants Giveaway (OGG), responsible for the business process of distributing a variety of medical grants designed to investigate multiple facets of community wellness, with the majority of grants disbursed to small hospitals, defined as having 250 beds or less. HBWC has a business process for collecting and storing the associated research data.

HBWC is planning to modernize the employee payroll and benefits management business process across the company through the use of an outsourced provider, such as Workday, ADP, or Peoplesoft. HBWC is also planning to upgrade its research database and develop a cloud-based grant tracking system. The company wants an analysis of the feasibility and planning for conversion to be added for consideration to the overall design for HBWC’s future infrastructure and services.

**Office of Grants Giveaway (OGG) Mission and Vision**

The mission of the HBWC’s OGG is to promote improvements in the quality and usefulness of medical grants through federally supported National Institutes of Health (NIH) research, evaluation, and sharing of information. The Small Hospital Grant Tracking System (SHGTS) is the primary application used to manage this data. Although the SHGTS contains hospital-specific banking data, grant funding is released via paper checks.

The SHGTS assists in the assignment and tracking of small hospital grants and is a single-user system running on a desktop computer. The OGG assigns a grant to one hospital for one month and then any unused grant funds are rotated to another hospital for the next month. The SHGTS tracks the initial delivery of the grant funds, stores pertinent information, and then follows the grant through the next five hospital facilities.

Only executive OGG staff can assign grant funds, but all principal investigators must complete their grant evaluations in the application. With the Paper Reduction Act, the federal government is moving their application from paper-based to an online submission system. Each week the OGG executive officer receives a grant status report. Each month, each principal investigator is briefed on the status of their current grants via reports generated by the SHGTS.

The OGG is expecting to receive more medical grants from the NIH and needs a way to grow the office’s staff while upgrading the infrastructure to support the current workforce, which consists of part-time workers, work-from-home employees, and contractors. As the OGG expands granting and resources for grant seekers, the creation of remote office branches to meet those needs is also being considered.

OGG is also collecting the requirements for a new, web-based portal for use by recipients of grants and researchers. This portal will contain patient-sensitive and other nonpublic information (NPI) that must be adequately protected during processing, storage, and transmission. Access to this resource will be managed by OGG staff with the appropriate privileged access.

HBWC’s current LAN administrator and security manager, who is responsible for most of the technology that is presently in place at OGG, is retiring next month. You have been promoted to assume this role upon the manager’s departure. Endothon Security Consulting completed a security assessment report (SAR) on behalf of the HBWC, therefore in your new position, you will be responsible for the following tasks

* conducting a thorough analysis of what’s in place technology—and applications-wise
* finding out which elements already in place are no longer able to support the operations
* synthesizing business, technical, security, and regulatory requirements for fitness in ongoing operations
* conducting a threat analysis of the applications and infrastructure to understand network and application security needs
* designing a replacement network to the existing LAN to support secure employee remote access, secure ACH data transmissions, secure NPI and patient data to the required levels and to support third-party extranet connections to cloud-based SaaS providers of services to OGG

HBWC is primarily Microsoft-based and wishes to preserve their relationship with Microsoft to ease migration from older-MS products to the newer suites of tools they offer (e.g., Office 365, SQL Server, ASP.NET). HBWC has a small staff of programmers needed to maintain existing applications and is fluent in C# and VB.NET. HBWC’s internet service provider (ISP) is Pogtech Communications, which provides broadband access for internal and planned external users of their resources and services*.*

**System Overview**

The SHGTS is a Microsoft Access 2010 database that resides on the Windows 2008 R2 application server. The SHGTS application and its data are protected by built-in security mechanisms supported by the hardened Windows 2008 R2 platform. Microsoft will stop supporting Windows 2008 in January 2020 and then Access 2010 in October 2020. This means that Microsoft will no longer supply patches for the software after 2020. MS Access is unsuitable for use by multiple simultaneous users and will need to be migrated to a MS SQL server with a new infrastructure. New access via the internet will also be required for sharing data among NIH, HBWC, and the hospitals they serve. A persistent link to NIH may be required to exchange data among multiple users and potentially multiple sites that might be needed for processing grants.

To segregate functions in support of SHGTS, three technical support personnel (members of the administrator group) have administrative rights to manage the Windows 2008 R2 server. The SHGTS database administrator (DBA) does not have administrative privileges to the Windows 2008 R2 operating system (OS).

The SHGTS database has been customized for group security to protect the application from design changes such as altering the visual basic for applications (VBA) code or modifying database objects. There are three categories of users for the SHGTS:

* **Administrative:** full control of the application, including the ability to alter code and modify database objects
* **Executive:** access to all reports and the ability to update key fields dealing with the assignment of grants
* **Basic:** access to most forms and the ability to update key fields relating to information about assigned grants

A virtual private network (VPN) firewall appliance is in place for users that require remote access to the SHGTS. Knowledge of the VPN is limited to users with a mission-essential need. Users access the VPN via Pulse Secure software using a token or a personal identity verification (PIV) badge.

Payroll is currently handled on HBWC’s premise using QuickBooks with paper checks. Direct deposit has not been implemented. Grant money is also provided by paper checks. Checks can be obtained from the office manager or sent through the mail.

HBWC’s patient information and other research data are kept in Excel spreadsheets. Patients have a patient number assigned to them throughout the research period and a conversion sheet between the patients and their associated numbers are also listed in Excel to maintain patient confidentiality. Principal investigators at each hospital are allowed to keep their data proprietary for one year while they are writing their research report. The NIH then becomes proprietor of all data. A hard copy of the research report is then saved in a file cabinet at the OGG and stored on the server. This makes it difficult for potential principal investigators to mine the data for information that could be used in future research.

**System Interfaces**

The SHGTS exchanges data with the NIH but does not give or receive any data to or from any other major application (MA) or a group system support (GSS). The SHGTS resides on Windows 2008 R2, but otherwise does not interface with any other system. It is accessed from local application running on HBWC workstations connected to the LAN. HBWC staff may access this database when they connect remotely through the VPN connection.

The HBWC uses a QuickBooks database for employee payroll, which is housed on the Windows 2008 R2 server and is a standalone database that can be accessed from the client workstations similar to the SHGTS.

The research raw data and reports are housed on the HBWC’s server in a fileshare.

**Data**

The SHGTS database contains private health information (PHI), other healthcare information, and proprietary data in its tables. Data stored in the SHGTS includes specific attributes about the grants such as control number, grant category, amount, distribution schedule, and sunset date. Information detailing grant distribution particulars, such as sponsoring staff, the directing official, and date assigned, is also stored in the system. The research data is only attributable to an individual if the conversion table is viewed along with the raw data.

QuickBooks contains personally identifiable information (PII) data on HBWC employees including social security numbers, salaries, home addresses, emergency contacts, phone numbers, and next of kin.

**Criticality**

The HBWC’s Information Systems Criticality Definition Processdefines automated information resources whose failure would not preclude HBWC from accomplishing core business operations in the short to long term (a few hours to a few weeks) but would have an impact on the effectiveness and efficiency of day-to-day operations being needed for daily processing of grants. The SHGTS also includes the research data, and the failure of the SHGTS would not preclude the HBWC from accomplishing core business operations in the short to long term (a few hours to a few weeks), but loss of the research data would require notification to NIH that the results of the research they funded is not available. However, failure of the system would have not an impact on the effectiveness or efficiency of day-to-day operations. Consequently, the SHGTS database is considered mission supportive.

Failure of the QuickBooks database could prevent employees from getting paid. A paper backup is maintained in case the server goes down, but the data may be a day old at minimum.

**Sensitivity**

The criteria used to measure a system’s sensitivity include confidentiality, integrity, and availability. The sensitivity areas for the SHGTS and QuickBooks are described below:

Confidentiality

*SHGTS: Low*

There is no Privacy Act or proprietary data to protect. No awardee information is tracked on the grants; the system only tracks grant-specific data. If unauthorized personnel read data that they are not authorized to see, administrative action (such as grant suspension or a letter of reprimand) would be the most severe consequence. If competing grant candidates discovered the grant rating system, the financial impact would be under $100,000.

*Research data: High*

The research data contains medical information on research subjects and needs to be compliant with HIPAA regulations and protected from employees that do not have a need to know. The research data also needs to be protected so that only the principle investigator can have access to it for the first year.

*QuickBooks: Medium*

There is Privacy Act data included in the QuickBooks database and the information should not be shared outside the payroll office.

Integrity

*SHGTS: Medium*

The data maintained on the grant ratings does affect recommendations for particular grants. Since entire medical research establishments use these recommendations, the financial impact of manipulated ratings could be between $150,000 and $300,000, but less than $1,000,000. Anyone involved with such data manipulation would possibly be sued but not sent to jail.

*Research Data: High*

The integrity of the research data must be paramount since the loss of data or any change in the data may show incorrect results of the research.

*QuickBooks: High*

The integrity of the data for salaries and other information regarding employees needs to be accurate to make sure that everyone receives the appropriate salary, based on job title and length of service.

Availability

*SHGTS: Low*

The reports are much easier to prepare with the database and it would be inconvenient if the database were unavailable to locate specific grants. However, manual inspection of invoices (for receipt information) and filed hard copies (to locate grants) could be used. The consequences of the database being unavailable would be viewed as an inconvenience but does not require a robust business continuity plan for continued access. The extra manpower required to manually prepare the reports would be less than $100,000 since, at worst, a contractor could be hired to prepare the most important reports for less than that amount.

*Research Data: Medium*

The research data does not need to be available 24 hours, but the information should be available when the principal investigator is preparing the final research report. A service-level agreement (SLA) and uptime schedule will be provided to researchers upon gaining approval to use the application.

*QuickBooks: Medium*

The information in the QuickBooks database needs to be available on paydays (every Friday). Hard copies are made of the information and stored in a filing cabinet, but that information may be dated.