Vbas® (Virtual Benefits Administration System)

Vbas® (Virtual Benefits Administration System) is a proprietary database BRMS developed to help streamline the administration of the benefit supply chain. By integrating this technology with our traditional services, we are able to further reduce healthcare costs for our clients. In fact, our customers have direct, secure access to control and manage all company data and benefit information. More importantly, employers have access to their employee benefit data anytime, anywhere.

In addition to eligibility, consolidated billing and reporting services, we also empower employers and employees to enroll online. While reducing paperwork, online enrollment helps eliminate errors and automates data transmission to insurance carriers. Employers can program benefit groups and categories for easy, online open enrollment. And with Insured Self-Service (ISS), employees can view and compare available plan descriptions, reference physician listings and add dependents. Online enrollment simply enables better tracking and management of employee benefit administration.

General Security

- Our servers are audited daily for all known security threats by ScanAlert.
- BRMS is open to allowing our clientele's personnel or third party vendors to perform network audits.
- BRMS agrees to share the results of any ASP audit with our clientele as it pertains to our clientele
- The application is stand alone except by the import and export functions requested by our clientele.
- ID, date, and time of all access are logged. Logs are kept for 12 months.

Network Security

- The web server is in a DMZ and the database server is on a trusted SBC network. Both servers are isolated from the rest of the SBC network via a firewall.
- Our network hosting application is air-gapped from any other network or customer that the ASP may have. Only the Vbas® application is hosted on this Web server and database server.
- Clients connect to the ASP via the Internet/world wide web using sign in and passwords required by Vbas®.
- BRMS utilizes security mechanisms sufficient in its sole discretion to protect the confidentiality and integrity of information provided by clientele and their employees. Security mechanisms used include, but are not limited to, encryption, access control mechanisms, authentication of electronic signature, physical hosting site security and firewalls.

Security measures taken at BRMS

BRMS will maintain electronic records on Vbas® pertaining to the use thereof by the company and its employees, including complete and accurate records of plans provided by company to its employees, records as to each employee's benefits effective date and termination date, amounts and types of coverage available to company and its employees under the plans and records regarding enrollment in plans.

BRMS will also maintain electronic records of transactions among BRMS, vendors, company and employees using Vbas®. Such records shall be maintained in accordance with generally accepted standards of electronic record keeping. It is the responsibility of company to download (electronically or on paper) company information from Vbas® prior to the termination. BRMS will not be responsible for storing copies of the company information for archiving or back-up purposes.

BRMS will maintain such electronic records in a manner accessible to company for a minimum period of twenty-four (24) months following the termination of said employee or plan.

The client will designate a single individual to act as the Principle User ("Principle User") for the company's use of Vbas®. BRMS will provide the Principle User with a password to access and use Vbas®. Principle User will have the ability to add, change or delete company information and any other information of company or its employees on Vbas®.

Principle User will have the sole authority to grant or delete Vbas® access privileges to company's employees, representatives and agents. The client is responsible for the designation of Principle User and shall notify BRMS immediately by written notice if they wish to designate a replacement.

The client is solely responsible for the activation and deactivation of access for its employees, representatives and agents. Other than access for Principle User, BRMS will not initiate, maintain or terminate access privileges unless requested in writing by an authorized officer of the company. The employer agrees to immediately notify BRMS if it becomes aware of: a) any loss or theft of any password, or b) any unauthorized use of any password, or c) any indication that anyone has or may have entered inaccurate, conflicting or inappropriate information into Vbas®.

Employee Access

The client is responsible for providing its individual employees with access to Vbas®. The company will create and provide each employee with an ID and password to access and use Vbas®. Each company employee will have access to company information intended for display to employees and selected information in the employee's own record.

Web Application Security — Signing by Electronic Means.

All Vbas® clients agree and authorize, on its own behalf and on behalf of its employees, that its/their electronic signature shall act as its/their formal signature for all Internet based transactions among the company, its employees, BRMS, vendors and any and all third parties. The client agrees on its own behalf and on behalf of its employees, to adopt as its/their signature, an employer identification code and a password, which is to be affixed to or contained in each transmission sent by such Party ("Signature"). While using Vbas®, the Principle User and Company's Employees will have the ability to change their password at any time. The client agrees and authorizes, on its own behalf and on behalf of its employees, that any Signature of Company affixed to or contained in any electronic document shall be sufficient to verify that the company executed such document and authorized the actions contemplated thereby. The client agrees and authorizes, on its own behalf and on behalf of its employees, that this Agreement, agreements ancillary to this Agreement and related documents to be entered into in connection with this Agreement will be considered signed when Signature of Company is transmitted electronically. Such Signature shall be treated in all respects as having the same effect as an original handwritten signature.

Security

- The ASP allows concurrent sessions
- 10 minutes is the session inactivity timeout
- Each session is initiated by the user unique within the application
- The ASP protects against application level attacks in the application environment with a unique randomly created page identifier passed between ASP pages. If a user attempts to circumvent the normal application process flow, an error will be displayed and the session will be terminated.
- The process the ASP utilizes for doing Quality Assurance security testing for the application is via a QA department that thoroughly tests the application, including its security measures.

Cryptography

- The ASP utilizes SSL, IPSec, and PGP encryption
- The ASP utilizes 128 bit encryption
- All connections to the ASP are protected using SSL and IPSec
- All pages are encrypted

Change Management

- When changes occur in the process, procedures or structure of our client's Vbas® account, an email will be sent.
- The ASP Change Management procedures address notification of the ASP Sponsoring Organization when changes are made to any resources impacting the client's application infrastructure.

SBC Hosting Overview

Our SBC PremierSERVSM Hosting solution is deployed in the world-class hosting environment of the SBC E-Services Internet Data Centers. The hosting environment is designed to meet the specific needs of our mission-critical operations. SBC E-Services Internet Data Centers, network and certified best practices enable a worry-free hosting experience, letting us focus our time and resources on our core business.

Disaster Recovery

Disaster recovery is part of the system. The application is "hosted" in an ASP model by SBC® Online Services, and as such they are responsible for addressing the majority of the disaster recovery plan. Additional information may also be found at www.sbc.com or www.webhosting.com.

This plan ensures the continuity of business in the event of a disaster, and provides for no more than one hundred twenty- (120) hour suspension of services.

Additional information on SBC outlines SBC® Online Service's capabilities in the area of off-site storage of all software and data necessary to operate all aspects of the system and the approximate time it would take to obtain equipment, software, materials, etc., to resume normal operations in the event of a major disaster such as a hardware system failure/collapse, a software system failure/collapse, a total loss of electrical power or any natural disaster.

SBC® Online Services is also responsible for conducting all regularly scheduled backups for our clientele's data and for the day-to-day computer-related processing operations. The SBC backup procedures are fully automated without operator intervention, other than to change backup media.

Information regarding where the backups are stored can be found on the SBC® Web site. To take the SBC® Online Services Virtual Data Center Tour, which covers a lot of the security and Disaster Recover resources, link to:

http://www.webhosting.com/media/SBC_Product_Virtual_Tour_RP.html.

Internet Data Centers

SBC E-Services Internet Data Centers were developed from the beginning with performance and reliability in mind. Their facilities are among the most hardened and secure available. SBC's vault-like security is supported by a number of advanced security technologies including digital video surveillance, digital asset tracking and biometric identification. The data center staff are technology experts and enable advanced hosting capabilities. They follow tested management processes to monitor software and hardware infrastructure on a 24 x 7 basis. The operating conditions within the facilities are fully managed. Advanced HVAC systems allow them to guarantee the environmental conditions, with fully redundant power, including back-up diesel generators, and ensure uninterrupted power sources.

Network

The entire network is designed to maintain high levels of performance and high availability. Redundant and diverse paths are used to avoid single points of failure within the IDC and provide optimal routing and traffic flow. For maximum performance and scalability, SBC E-Services Internet Data Centers are connected to the Internet by redundant OC-12 circuits that are scalable to OC-192 capacity. For further reliability and redundancy, each data center has dual path, dual-entry fiber facilities and is served by two different central offices.

Network highlights

- SBC monitors for new vulnerabilities on a regular basis.
- Fully meshed and redundant networks powered by Cisco products
- Dual-entrance and dual path OC-12 access scalable to OC-192 capacity
- Advanced capacity monitoring and planning for scalability
- Proactive 24 x 7 x 365 monitoring and management by certified staff
- Managed Firewall solutions including configuration, installation and ongoing management, as an added layer of security
- Comprehensive SLAs
- ASP, Javascript, ActiveX. is used for the application environment
- Vbas® Version 2.0 and Microsoft Windows Advanced Server 2000 will be utilized for the application environment
- Visual Basic is the language the application the back-end is written in

Managed Servers

Our dedicated servers run on Microsoft Windows 2000 Advanced Server.

System Monitoring — SBC's data center staff monitors a number of health and performance statistics on our individual system

We have 24 x 7 guaranteed peak performance. SBC's Operations Service Center (OSC) monitors all systems within our hosted environment including performance levels, availability and resource utilization.

System Maintenance — In addition to monitoring our systems, SBC's OSC performs routine maintenance on all system components, as needed, allowing them to predict service impacting problems before they occur. In the unlikely event of a failure, the support team will address it quickly and efficiently.

Optimized Software — Pre-engineered, tested operating system builds to ensure security, performance and availability

Optimized Hardware — Pre-configured, hardened server hardware from HP.

Reliability, performance, security

- Runs custom applications
- Data security
- Data reliability
- Handles high user traffic conditions
- Server handles heavy content and script load
- Control over server environment and configuration
- Server will perform multiple functions such as FTP, mail and web server

Monitoring Services

SBC provides 24 hours, 7 day a week monitoring for our servers.

Disaster Recovery

SBC E-Services offers services from Tape Back-Up, available with each server to back up our data on a daily, weekly or monthly basis to a full DR service. A plan is in place that covers our servers, applications, processes, network, and personnel to limit our downtime. We have Tape Back-Up, a managed Storage Area Network solution and Dedicated Array Storage.

Bandwidth

We have unlimited bandwidth.

Software is installed with Windows 2000/2003 server

Windows 2000/2003 servers come with a standard installation of Windows Server, with the latest IIS (6.0) and service pack. We have administrative access to the server through PCAnywhere. We have root control and can install any additional software we like on our server (database, e-commerce, etc), within usage guidelines.

Certifications & Compliances

SBC E-Services has external organizations audit operational practices, including security processes.

SBC E-Services employs industry best practices and receives certifications from some of the industries leading authorities. SAS70 is an accounting standard developed by the American Institute of Certified Public Accountants. It measures the design and operating effectiveness of the controls affecting the operational and administrative functions at the data centers. The audit reviews both the physical security and logical access with respect to the SBC E-Services IDCs.

The physical security review verified that the controls in the SBC E-Services IDCs provide the reasonable assurance that administrative and operational procedures are established to ensure protection of physical assets. The logical access review considered whether the controls provide reasonable assurance that logical access to data, system software, hardware, and system utilities are restricted to properly authorized individuals and programs.

HP SP Signature Certification covers a service provider's IT infrastructure and its ability to support the delivery of quality services. The assessment reviews in detail four domains of availability of the IT infrastructure:

- Network
- System software
- Hardware
- Environment

Furthermore, the Signature Certification includes a comprehensive assessment of people, process, and technology and provides recognition of the service provider's capability to consistently deliver a reliable service to a defined standard based on industry best practices. In order to maintain industry best practices, service providers conduct an annual re-certification process.

SunTone certification demonstrates that a given service has met stringent requirements for availability, reliability, performance, scalability, and other quality measures. The key components of the SunTone are:

- Validation of the data center service against the industry driven standards of the SunTone Service Delivery Specification and SLAs.
- Technical guidelines detailing processes and policies for architecting, implementing, and managing networked services.
- Reference Architectures for enabling customers to quickly build integrated, tested, tuned, and documented architectural implementations.
- SunTone certification signifies quality data center service offerings.

Physical security measures taken at the SBC Data Center

We take security very seriously. Every precaution is taken to ensure that no one has access to our server other than SBC's certified Internet Data Center technical staff. SBC staff even has to pass through security measures to access our server. Passkeys and video surveillance ensure that our server is safe and secure.

Feature	Biz Pack
	HP Server Option
Server	HP DL-360 G4
Number of Servers	1 or 2
Processor Speed	Xeon 3.0 GHz
# of Processors (base package)	1
RAM (MB)	1024
Hard Drive (GB)	(1) 72 GB 10K RPM SCSI
RAID	1
NIC	(2) 7170
Operating System	Linux 3.0 or Windows 2003
Web Server	IIS or Apache
Firewall	NetScreen 5GT dedicated
Switch	Cisco 2950-24 (for 2 servers only)
Tape Backup	A10 with VERITAS NetBackup (10 GB / month)
Monitoring	Lite Monitoring
Included Email Boxes	20
IP Addresses	1
DNS Service	Included
Data Transfer / Mo.	100 GB
Data Transfer above limit	$5 / GB
Tape back up	A100 w/ 100 GB/month