Security Components of HBSS Co-Location Hosting Services		
Component Title	**Description**	**Solution**
Identification and Authentication	Supports obtaining information about those parties attempting to log onto a system or application for security purposes and the validation of users	HBSS has a click-stream audit log. All user actions are tracked and logged.
Access Control	Supports the management of permissions for logging onto a computer or network	HBSS has a user role-based access management module
Encryption	Supports the encoding of data for security purposes	All HBSS software and websites are HIPAA compliant and implement 128 bit encryption as well follows all HIPAA specified security protocols.
Intrusion Detection	Supports the detection of illegal entrance into a computer system	HBSS uses and maintains a firewall, with latest patches to protect its private network from the Internet. HBSS configures the firewall to reject all incoming traffic not deemed necessary for business operations. This means closing access to all unnecessary Internet services. HBSS performs penetration testing on the firewall at least four times a year to disclose any new vulnerabilities. HBSS reviews the results of the penetration tests, mitigates any of the vulnerabilities found and re-scans the firewall once necessary changes have been made. HBSS shall install and configure an IDS to monitor all traffic outside the firewall. The IDS logs will be reviewed on a regular basis. If an attack is detected, network administration will be notified and corrective action taken.
Verification	Supports the confirmation of authority to enter a computer system, application, or network	HBSS portal validates the user before allowing access; Network is secure.
Digital Signature	Guarantees the unaltered state of a file	HBSS implements digital signatures via password, and will guarantee the state of files.
User Management	Supports the administration of computer, application, and network accounts within an organization.	HBSS has a web based account management system which is restricted to admin users only. This screen is used to create, delete, modify database and application accounts, and privileges.

		HBSS uses a Windows provided user account management system for computer accounts. The network equipment accounts are managed directly with the various vendor provided account management screens.
Role/Privilege Management	Supports the granting of abilities to users or groups of users of a computer, application or network	HBSS has a user role based access management module.
Audit Trail Capture and Analysis	Supports the identification and monitoring of activities within an application or system	HBSS has a click-stream audit log. All user actions are tracked and logged.
Input Validation	Ensures the application is protected from buffer overflow, cross-site scripting, SQL injection, and unauthorized access of files and/or directories on the server.	Buffer Overflow and Code Injection Prevention: HBSS uses .NET for programming, which is strongly typed and checks array bound violations. HBSS programmers perform thorough input validation and constrain input by validating it for type, length, format, and range. HBSS software does not used unmanaged code or APIs. All APIs are wrapped in managed code. HBSS uses the /GS flag to compile code developed with the Microsoft Visual development system. The /GS flag causes the compiler to inject security checks into the compiled code. This tight input validation also prevents code injection, as all input validated for type, length, format, and range. Cross-Site Scripting Prevention: All HBSS web applications ensure that input from query strings, form fields, and cookies are valid for the application. HBSS considers all user input as possibly malicious, and filter or sanitize for the context of the downstream code. HBSS validates all input for known valid values and then rejects all other input. HBSS uses regular expressions to validate input data received via HTML form fields, cookies, and query strings. HBSS also strives, where needed, to use HTMLEncode and URLEncode functions to encode any output that includes user

		input. This converts executable script into harmless HTML. SQL injection Prevention: HBSS web applications validate input prior to sending a request to the database. HBSS uses parameterized stored procedures for database access to ensure that input strings are not treated as executable statements. When HBSS cannot use stored procedures, HBSS uses SQL parameters when building SQL commands. HBSS uses least privileged accounts to connect to the database. Unauthorized Access to Directories and Files: Our web servers run IIS7 and higher and we apply all the latest patches as when released by Microsoft. The database is SqlServer 2005 or higher and patches are applied as and when released by Microsoft. The web Server does not allow access to directories and files.