ATTACHMENT 25:

NYS DOH HCS INTERNET APPLICATION DEVELOPMENT GUIDELINES

NEW YORK STATE, DEPARTMENT OF HEALTH

OFFICE OF LONG TERM CARE

UNIVERSAL ASSESSMENT TOOL

FAU 1005130955

Table of Contents

A HCS Integration

The purpose of this document is to provide information for NYS DOH contractors or vendors who will be developing and/or hosting web-based internet applications in the NYS DOH Health Commerce System.

The NYS DOH has created a web site on the Internet for use by the Department's public health partners and customers. This web site is located at https://commerce.health.state.ny.us (note the "s" following the http) and is referred to as the Health Commerce System, or HCS.

The Bureau of Healthcom Network Systems Management (BHNSM) at the NYS DOH is responsible for design, development, implementation, management and operation of the NYS Health Commerce System. The Health Commerce System is an enterprise wide secure internet system with over 100 critical applications and 50,000 users in 13,000 organizations in local, state and federal levels.

A.1 BHNSM Preferences

BHNSM favors certain technologies and open standards including the following:

1. Non-proprietary Web service specifications that promote interoperability among Web services such as Web Services-Interoperability (WS-I) Basic Profile and Basic Security Profile (WS-I BSP).
2. Protocols that facilitate the secure exchange of authentication and authorization information between partners regardless of their security systems or e-commerce platforms. Security Assertion Markup Language (SAML) tokens
3. Oracle database technology with standard data access components is the preferred platform and implementations that do not incorporate proprietary vendor extensions for database access.
4. JEE (Java Enterprise Edition) application approach that offers compatibility and can be easily distributed.

A.2 User Sign-In, Authentication, and Security

Each person who requires access to the HCS and one or more of its applications is required to apply for a user ID and password and provide the appropriate security-related attestations (see *Attachment 23 Security Requirements V 3-1-2009 09-10.pdf*). Once a person has a user ID and password, they go to the HCS web address (https://commerce.health.state.ny.us) and enter their login ID and password.

If the user ID and password are valid and authenticated, the HCS provides the user with a web page that includes a list of all of the applications the user has the authority to use. The UAT solution will be one of those applications. No additional login procedures are necessary.

This "single sign-in" procedure benefits users by simplifying their access to multiple NYS DOH applications. It also ensures that users whose access to an application should be revoked can be removed from the system properly and easily.

Per the User Administration and Login requirements described in the core functional requirements section of the RFP, there will be a coordinated effort between the UAT solution and the HCS for granting access and defining user rights.

Note: No user ID and password should be provided directly to any database. Database access should be conducted through the application for which a user has authority.

The security system employed on the NYS DOH commerce site is known as the Web Access Authentication Routing Proxy (WAARP). WAARP is a "reverse proxy" with an authentication API; it is the WAARP system that authenticates a user, checks that user's authorization for an application, and allows (or does not allow) the user to run the application.

In order for WAARP to recognize that a user is requesting access to a WAARP controlled application, conventions for the URL and placement of the application's files on the server must be followed.

Application vendors must conform to New York State guidelines for security and user authentication. See Best practice Guideline G07-001 that defines Identity and Access Management: Trust Model Guidelines.

See *Attachment 28 NYS Identity and Access Management Trust Model.pdf.* Also refer to the security requirements section of the RFP.

A.3 Application Identification

For the purposes of WAARP, an "application" is specifically defined as a function or functions accessed on an application server with access restrictions on which users may access those function(s). All applications, and user access to these applications, must be registered with WAARP.

All applications are identified within WAARP by an alphanumeric string of 8 characters or less, which is referred to as the "application ID." For example, the application ID for an electronic assessment system could be: UAT. Information concerning this application would be stored in the WAARP database.

The selected development vendor will work with BHNSM staff to determine the permission class, permission values, and permission types for the application. These values determine user access to the data and the applications and will be explained in detail to the selected development vendor during the analysis phase of the project.

These values will be used in conjunction with the user ID and permissions configured within the UAT solution. See the section titled User Administration and Login in the core requirements section of the RFP for more information.

When the application is run, the WAARP system reports back to the application the permissions which were granted to the user who is running the application. The WAARP system has no knowledge of what an application's permissions mean, it is merely reporting the user's permissions to the application, and it is the application's responsibility to act correctly upon those permissions.

Finally, a contact person at NYS DOH will be designated as the person responsible for creating and maintaining the application's permissions within WAARP. This will be described on as as-needed basis to the selected development vendor.

Applications retrieve variable information from its runtime environment via cookies. WAARP provides the variable information in the user's cookie by the HTTP_COOKIE environment variable. The details of the cookie will be provided on an as-needed basis to the selected development vendor.

A.4 Database Access

User access to the data in the database is achieved through the application, which is governed by WAARP. No user should have direct access to the database.

Application access to the back-end database is achieved by using the *application* ID and password that the WAARP system has put in the application's environment (described in the previous section).

As noted in the Security Requirements secion of the RFP, this is the only allowable method by which the application, and therefore a user, may connect to the database.

Applications must *not* use embedded user ID and password information, and individual users must not be given IDs and passwords for the database.

Database applications must use ANSI standard SQL on the back-end RDBMS and database independent connectivity methods such as JDBC, Perl DBI, or ODBC.

A.5 HCS Web Server Technologies

Application support on NYS DOH's HCS exists for the following applications, databases, and operating systems:

- Perl CGI
- J2EE applications written using BEA's WebLogic Application Server
- SAS
- SUN Solaris
- Netscape/IPlanet Commerce Server
- Sybase or Oracle RDBMS

Examples of current applications running on the NYS DOH HCS web server are:

- Data file uploads using the file upload feature of web browsers
- Dynamic queries created using Perl/HTML, with queries being submitted by SAS Access. SAS then creates graphs/reports from the output and returns the results to the client.
- Data entry and query applications using Perl/SybPerl/HTML
- Data entry and query applications using J2EE

A.6 Client Requirements

Because the NYS DOH HCS only supports web-based applications, users access the site and its applications using web browsers.

The NYS DOH HCS site is running http over SSL 3.0 (https on port 443) with 128-bit encryption.

Client web browsers must also support 128-bit encryption (freely available with versions of Netscape Communicator and Microsoft Internet Explorer, both of which support 128-bit encryption).

A.7 Best Practices in Internet Application Design

Applications must not allow the user to type in any command that would be executed directly by the application, database, or operating system.

Some references for designing internet applications include:

- The CERT (Computer Emergency Response Team) Coordination Center: http://www.cert.org
- The World Wide Web Security: http://www.w3.org/Security.

For detailed security requirements, see *Attachment 21 Security Requirements V 3-1-2009 09-10.pdf.*

A.8 Compliance with New York State Technology Standard

The proposed and final candidate solution must conform to P08-005 Accessibility of Web-Based Information and Applications, which defines accessibility of State Agency Web based Intranet and Internet Information and Applications.

See *Attachment 27 P08-005 Accessibility of Web-Based Information and Applications.pdf.*

A.9 Solution Guidelines and Standards

NYS DOH advocates standards and guidelines intended to establish uniformity in common technology infrastructures, software applications, processes and data integrity across the DOH and other state agencies. The following list represents technologies and solutions which are compatible with New York State standards and guidelines.

1. Solutions which are open, standards-based, vendor neutral, scalable and are capable of meeting the state's current and future needs.
2. Solutions that have been subjected to successful validation and verification tests to ensure the openness of its key interfaces.
3. Solutions that ensure that the privacy of transactions and stakeholder data will be guaranteed and compliant with all state regulatory requirements and best practice recommendations.
4. Solutions that can be centrally managed and are easily configured.
5. Solutions that allow interoperation with various open standard products in the market including but not limited to HTML, XML, HTTP, TCP/IP, SSL, PKI, JEE, JSP, EJB, Enterprise Java APIs.
6. Solutions which incorporate Services Oriented Architecture (SOA) and web services architectures.
7. Traditional web-based solutions that employ a thin-client, middleware, and backend database architecture.
8. Document-centric solutions that will make use of the State's enterprise content management (ECM) architecture, including its content repository, business process and workflow management tools. NYS DOH currently utilize FileNet P8 platform suite of products.

A.10 Communications Directory

The Communications Directory is a central repository that supports the creation and maintenance of user profiles. User profiles include such information as professional profile, multiple contact information, association with facilities or organizations, user roles, communication preferences, and security related authority and access rights to applications.

NYS DOH anticipates that the Communications Directory will be able to provide the following functionality to support the universal assessment process:

- Ability to administer user profile information including name, street address, city and zip, contact details, preferred mode of communication, license number, associated facilities, and other professional information.
- Ability for a system administrator to assign one of the default profiles to a specific user when their account is established or when their job function changes. The result will be that the user will inherit the rights associated with the default profile.
- Support for the creation of institutions and individuals who may not be active assessment participants but who may need to be referenced by the UAT solution for the purpose of notifications or completing information in an assessment.
- Allow users to be associated with a valid institution (for example, a specific hospital, funeral home, physician practice, county office) even if the institution is a single person business entity.
- Provide for the creation and configuration of user roles (funeral director, medical certifier, hospital clerk) that can be easily assigned when creating new or modifying existing users. These pre-defined roles would contain completed authorization matrix and profile settings that would be inherited by a new or existing user.
- Ability for users to have an association with more than one institution with differing roles for each institution.

A.11 HCS Notification Capabilities

The NYS DOH HCS provides support for communications between HCS applications and individual users, as well as between individual users of an application. The HCS Notification capabilities support communication to users via phone, pager, fax, and email. A user's preferred communication method is maintained as part of the user's profile in the . The notification capability utilizes information contained in the Communications Directory such as role and contact information and supports predefined or user customized lists. Health Commerce System provides an XML interface to allow business application developers to integrate with this notification capability to provide the type of extended notification requirements defined in this RFP to support New York State universal assessment.