

EXHIBIT

MSDH Standard Database Design Lifecycle

Mississippi State Department of Health (MSDH) Office of Health Informatics (OHI) Information Resources Management Database Administration (IRMDBA) group requires all vendor COTS and in-house databases to graduate through a design lifecycle migration path that moves from TEST, to QA, to PROD database instances. This applies to both Oracle 9i and Microsoft SQL Server 2000 databases.

- **TEST**
The TEST database environment is where technical database designs are developed and tested. This includes the structure, data, and data handling functions. The structure includes all relational database objects, such as schemas, tables, columns, column types and sizes, partitioned tables, indexes, partitioned indexes, primary and foreign key constraints, triggers, sequences, stored procedures, functions, packages, XML structures, user-defined object-oriented structures, SQL queries and scripts, PL/SQL routines, data dictionaries, data migration and loading scripts and utilities, etc. Iterative changes to the schema will be made only in the TEST instance. Only after the technical parties involved, such as the developers, DBA's, vendors, managers, etc have agreed that the design is complete and working properly will the database be migrated to QA. This migration will occur via an export (Oracle) or backup (MS SQL Server) transfer. A hard-copy sign-off sheet is required to authorize this migration.
- **QA**
The database is either imported or restored (from backup) into the QA instance. QA is where the functional owners of the application test the functional readiness of the project. This includes local, remote, and field testing. Nothing, except data, is ever changed in QA. Any enhancements, modifications, improvements, additions, or changes to the database schema that result from QA testing are made in the TEST instance. Once again, for each and every structure change that result from QA or pilot testing, these changes are re-tested in the TEST database for technical correctness before they are migrated up to QA via an additional hard-copy authorization sign-off form. Any subsequent new changes are required to go through this TEST-to-QA cycle again. We do not deviate from this requirement.
- **PROD**
Once all involved parties agree that the database design has been thoroughly tested and qualified in QA, it is then exported or backed up and migrated to PROD via a hard-copy authorization sign-off form. Nothing, except data, is ever changed in PROD. PROD is locked down in secure, reliable, and responsive production datacenter servers that are up and available 24x7x365 and are backed-up on a nightly basis for fast recovery.

Database Requirements

1. Database Requirements

- a. Microsoft Database designs will be based on the Oracle 9i Database Enterprise Edition (9.2.0.1.0 with latest patches) with Advanced Security Option core technologies or the SQL Server 2000 (8.00.760) with Service Pack 3.
- b. Vendor will comply with the MSDH Standard Database Design Lifecycle that includes the Test, QA, and Production environments and migration paths.
- c. Central Office databases will reside in a central server instance of Oracle or Microsoft SQL Server 2000 that is physically located on the MSDH internal data network, administered by MSDH personnel, and separated from any client/server or web-based application.
- d. The database schema design is required to be truly relational and take full advantage of all available Oracle 9i Relational Database Management System (RDBMS) or SQL Microsoft Server 2000 objects, such as partitioned tables, partitioned indexes, stored procedures, packages, package bodies, triggers, sequences, functions, the XDB database structure, and others.
- e. The database schema design is required to be normalized to third-normal form.
- f. The database schema design must support meaningful data extraction and reporting operations using standard Structured Query Language (SQL) statements.
- g. The relational schema cannot be used just as a repository of flat tables, reference tables, or control table structures that simply support intermediate layers or “metalayers” of business-rules or application logic.
- h. The database schema design will use the standard Oracle 9i RDBMS or Microsoft SQL Server 2000 relational features, such as primary keys, referential integrity constraints (foreign keys), and unique keys, to enforce and maintain transactional data integrity.
- i. All schemas and associated Data Definition Language (DDL), Entity Relationship Diagrams (ERD), Data Dictionaries, and Data Models will be developed with Entity Relationship for Windows (ERWin by Computer Associates, Inc.) only. Visio or other ERD modeling tools are not acceptable. This required version of ERWin must be completely compatible with ERWin 4.1.2771, which the MSDH standard.
- j. Automatic or dynamic schema development, changes, or modifications by

machine-generated or software-generated code will not be allowed. Every addition, modification, or change to the schema or any database object will be modeled using ERWin and is required to graduate through revision and configuration management control and be thoroughly documented and approved before implementation.

- k. Vendor must purchase their own ERWin licenses.
 - l. Vendor will use an integrated database design toolset that includes source code control management, configuration management, and a web-based bug tracking/resolution system that is accessible by MSDH personnel.
 - m. The Oracle 9i database must be capable of residing on and taking full advantage of both Microsoft Windows 2003 and Sun Microsystems Solaris 2.9 servers.
 - n. Vendor will work closely (on-site) with MSDH Database Administrators to design the schema.
 - o. All schema development will occur at the MSDH Office of Health Informatics.
 - p. All database administration functions will be administered and executed by MSDH Office of Health Informatics Information Resource Management DBA's.
 - q. Vendor will participate in design review meetings every two weeks.
 - r. MSDH personnel reserve the right to ask any technical question and request any technical documentation that may arise from any sales presentation, functional demonstration, technical demonstration, or communication related to the Vendor's products or services.
 - s. Vendor will provide answers to technical questions and requested documentation prior to the contract award.
 - t. Vendor will comply with the MSDH Database Design Documentation Guidelines
 - u. Vendor will comply with the MSDH Oracle Coding Standards.
2. DATABASE USER ACCOUNTS – Accounts for each individual database user.

Every person who connects to the database will have their own account that will be auditable. The only way that a user can be truly audited is for the user to use their own individual database login account. Individual users will not be allowed to share accounts or use any generic account. These accounts will have only the CONNECT role privileges that include only select, insert, update, and delete of data rows. Other privileges or functions, such as truncate table, will be granted on an as-needed basis. User accounts will not be allowed to have database administrator (DBA) roles or ADMIN, SA,

SYSTEM, SYS, SYSDBA, or SYSOPER system privileges grants in any MSDH database environment. All account passwords are required to be encrypted. Please see the PASSWORD MANAGEMENT section below for more about passwords.

- a. SCHEMA-OWNER ACCOUNTS - Accounts under which the database schema is built or created.

Schema-owner accounts will not be allowed to have database administrator (DBA) roles or ADMIN, SA, SYSTEM, SYS, SYSDBA, or SYSOPER system privileges. They may have the RESOURCE, IMP_FULL_DATABASE, and EXP_FULL_DATABASE roles only in TEST. They may have only the IMP_FULL_DATABASE role in QA and Production. All account passwords are required to be encrypted. Please see the PASSWORD MANAGEMENT section below for more about passwords. For Microsoft SQL Server 2000, the database owner user can have DBO privileges but not SA privileges.

- b. OTHER ACCOUNTS

Persistent-database-connection accounts, such as those for web services or connection pooling purposes, will be granted only the CONNECT role. All account passwords are required to be encrypted. Persistent-database-connection accounts will not be allowed to have database administrator (DBA) roles or ADMIN, SA, SYSTEM, SYS, SYSDBA, or SYSOPER system privileges grants in any MSDH database environment. Please see the PASSWORD MANAGEMENT section below for more about passwords.

3. PASSWORD MANAGEMENT

The following policy applies to all database account passwords used on OHI platforms.

- a. Will be composed of an eight (8) character string that includes a combination of lower and upper case alphanumeric characters and the numerals 0-9.
- b. Will be encrypted.
- c. OHI Database administrators will control all aspects of passwords.
- d. Have a life of 90 days. Will expire in 90 days.
- e. Three (3) attempts to log in with an invalid password will lock a user out.
- f. Change history will be logged and recorded
- g. Can never be reused.