

Secure Enterprise Access to Support Collaboration on Clinical Research

Oracle9iR2 Database Security

Oracle World, Sept. 9, 2003

Nitin Sawhney, Ph.D.
Cal Collins and Tom Hickerson

Akaza Research, Cambridge, MA
<http://www.akazaresearch.com>



Psychiatric and Neurodevelopmental Genetics Unit
Massachusetts General Hospital
<http://pngu.mgh.harvard.edu>



Outline of Talk

- PhenoDB: Phenotypic Data Repository for Clinical Research
 - » Collaboration for Clinical Research
 - » Approach and Deployment
 - » Clinical Research Settings: Key Design Challenges

- HIPAA Regulations and Standards
 - » Privacy Rules and Security Standards
 - » Implications for Database Applications

- Oracle Security for Clinical Research Settings
 - » Selective Data Encryption
 - » Oracle Label Security
 - » Oracle Auditing



Collaboration on Clinical Research for Rare Disorders

- Clinical studies on genetic causes of rare psychiatric disorders such as Schizophrenia, Autism and Tourette Syndrome
- Collaborative research among investigators at Mass General Hospital, Whitehead and various academic institutes worldwide
- Studies require collection of both phenotypic (exhibited traits) and genotypic (genetic makeup) data on afflicted individuals & families
- Challenges: collect bulk legacy & longitudinal data from distributed sites, handle complex metadata, and enable statistical analysis
- Key Objective: To gain insights on complex phenotypes that characterize rare disorders

Oracle World : Sept 9, 2003 : 3 :: 23



PhenoDB: Phenotypic Data Repository

- Pilot Project: Support international consortium of researchers investigating Tourette Syndrome – led by Dr. David Pauls, Harvard Medical School
- Centralized repository to securely manage data and provide integrated data analysis for cooperative research (distributed online access)
- Import bulk legacy clinical data, integrate with genotypic data and export to various analytic formats
- Dynamically generate various existing and custom psychiatric evaluation instruments and query tools from predefined metadata
- Manage hierarchical projects and roles, while providing intuitive workflows
- Deployment:
 - » Sun Fire V480 Server running Solaris 8
 - » Oracle 9iR2 database, behind Partners VPN firewall
 - » Java J2EE framework and Tomcat webserver

Oracle World : Sept 9, 2003 : 4 :: 23



PhenoDB Interface: Data Submission and Query

The screenshot displays three overlapping windows from the PhenoDB interface:

- Top Window (Login):** Titled "Login to PhenoDB", it features a "User ID:" field and a "Password:" field.
- Middle Window (Query Library):** Titled "Query Library: Create or Select Queries", it includes a "Create a New Query" button and a table of existing queries.

ID	Name	Description
<input type="checkbox"/>	007 test of new report format	looks for external project id
<input type="checkbox"/>	208 test of s001 and s002	test of query for skings
<input type="checkbox"/>	215 test 25 and test 75	test of some outliers
<input type="checkbox"/>	222 00001 and 004 75	we will see if two and want both have 3 in the out
<input type="checkbox"/>	223 looking at 00001 or 002 > 0	Looking at some of these traits may lead to falsi
- Right Window (Data Entry):** Titled "PhenoDB: Enter Phenotypic Data", it shows a confirmation message "Your changes were inserted into the database." and a list of data points:
 - Project: TS-5b Par
 - Family: 041
 - Instrument: TS-5b Par Self Report v1.5.0
 - Individual: 000-001-01
 - Status: Currently being collected

Oracle World : Sept 9, 2003 : 5 :: 23

PhenoDB Interface: Data Validation

The screenshot displays the "PhenoDB: Validate Phenotypic Data" page. It includes the following elements:

- Header:** "PSYCHIATRIC & NEURODEVELOPMENTAL GENETICS UNIT" with navigation tabs for Home, Select Phenotypic Data, Family Data Entry, and Administer.
- Message:** "There are some discrepancies in validating this data. Please look below and update them as necessary."
- Metadata:**
 - Project: TS-5b Par
 - Family: null
 - Instrument: ESACG VT v.1.2
 - Individual: 010-003-02
 - Status: already complete
- Section: Depressive Disorders**
 - Pages in this section: 52
 - Page 13 - [back to top](#)
 - Current findings of depression based on verbal complaints of feeling depressed, sad, down, like crying
 - 13. Overall: 0 - No Information
 - 14. Summary: 0 - No Information
 - 14. Parent: 1 - Not at all
 - Note: "Your answer to this question is different than what was originally entered. The original answer was: 0. Please re-check your actual response and enter it."
 - Next findings of depression based on verbal complaints of feeling depressed, sad, down, like crying
 - 15. Past Child: 0 - No Information
 - 16. Past Summary: 0 - No Information
 - 17. Past Parent: 0 - No Information
- Comments:** A text area with the label "COMMENTS: 9-2".

PhenoDB Interface: Managing Clinical Studies

PHENODB: Status of Submission

Your changes were inserted into the database.

Section	Questions Entered	Questions in Section	Data Entered	Validation
Motor Tic Checklist	0	135	Not Completed	Not Completed
Phonic Tic Checklist	0	50	Not Completed	Not Completed
Description of Multiple Tics	4	4	Completed	Not Completed
Current Severity of Tic Symptoms	0	0	Completed	Not Completed
Worst Ever Severity of Tic Symptoms	0	0	Completed	Not Completed
Age At Onset	15	15	Completed	Not Completed
Obsessive Compulsive Checklist	0	451	Not Completed	Not Completed
Worst Ever Severity of Obsessive Thoughts and Compulsive Behaviors	0	5	Not Completed	Not Completed
Age At Onset, Obsessive Thoughts	0	5	Not Completed	Not Completed
Age At Onset, Compulsive Actions	0	5	Not Completed	Not Completed
Help Sought Obsessive Thoughts and/or Compulsive actions	0	7	Not Completed	Not Completed
Attention Deficit Hyperactivity Disorder Checklist	0	85	Not Completed	Not Completed
Medications Taken Currently or in Past	0	132	Not Completed	Not Completed

This instrument is **incomplete** for this individual.

[Click here](#) to return to the Collect Data menu.

PhenodB Prototype - August 20, 2009

Challenges for Databases in Clinical Research Settings

- Ensuring a **robust, scalable and extensible system** for distributed usage at research sites worldwide
- Providing **intuitive** query, data entry and administrative tools for use by investigators and clinicians
- Generalizable for **diverse clinical studies** in a centralized database
- Enabling **bulk data import** from legacy sources like Access & KP5
- Ensuring **double validation** of data submitted and auditing
- Access for **hierarchical roles, privileges & data sensitivity levels**
- Compliance with **HIPAA regulations & guidelines**

HIPAA Regulations and Standards

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
 - » Goals: Privacy, Security, Standardization and Efficiency in Healthcare*

- Administrative Simplification Provisions
 - » Electronic transactions and code sets standards
 - » **Privacy requirements**
 - » **Security requirements**
 - » National identifier requirements

- Key Challenge
 - » Providing reasonable Security & Privacy while ensuring adequate performance and minimizing administrative overhead?

* <http://www.cms.hhs.gov/hipaa/>

Oracle World : Sept 9, 2003 : 9 :: 23



HIPAA Privacy Rule for Clinical Research

- Privacy Rule limits release of “protected health information” (PHI) without patient’s knowledge and consent

- Applies only to “covered entities” which may include healthcare groups, organizations & businesses that handle PHI

- Researchers may not be covered entities, unless they are also health care providers who electronically transmit PHI during studies

- PHI considered individually identifiable information e.g. Name, Date of Birth

- Covered entities may disclose PHI without restriction, if it is de-identified

- Covered entities should seek individual’s written permission for use of PHI for research purposes

Oracle World : Sept 9, 2003 : 10 :: 23



HIPAA Rule on Security Standards

- Security standards to safeguard the "confidentiality, integrity and availability" of electronic information used in health care
- Final rule published on Feb. 20, 2003 and only applies to covered entities*

Key Provisions:

- General Rule Provisions
- Administrative Safeguards
- Physical Safeguards
- **Technical Safeguards**
 - » Access control policies - unique user ID, auto logoff, encryption of PHI
 - » Transmission security - integrity controls & encryption (not over open networks)
 - » Audit controls – hardware, software and procedural methods
 - » Person Authentication – ensure person seeking access to PHI is who they claim

* <http://www.hipaadvisory.com/regs/finalsecurity/summaryanalysis.htm>

Oracle World : Sept 9, 2003 : 11 :: 23



Data Privacy and Security: Implications of HIPAA

- **Authentication**
- **Integrity**
- **Authorization**
- **Availability**
- **Confidentiality**
- **Auditing**

Oracle World : Sept 9, 2003 : 12 :: 23



Data Privacy and Security: Utilizing Oracle9iR2 Features

- **Authentication** → *SSL & Single Sign On*
- **Integrity**
- **Authorization** → *Oracle Label Security*
- **Availability**
- **Confidentiality** → *Selective Encryption*
- **Auditing** → *Oracle Auditing*

Oracle World : Sept 9, 2003 : 13 :: 23



PhenoDB: Oracle Privacy and Security Approaches

- **Selective Data Encryption**
- **Oracle Label Security**
- **Oracle Auditing**

Oracle World : Sept 9, 2003 : 14 :: 23



Selective Data Encryption

- PL/SQL Package to encrypt/decrypt stored data
 - » DBMS_OBFUSCATION_TOOLKIT
 - » Support Bulk Data Encryption using DES, 3DES or MD5

- For Clinical Research, Encryption useful for:
 - » User Passwords
 - » Place of Interview
 - » Date of Birth (DOB)
 - HIPAA considers DOB individually identifiable, but researchers require it for their clinical studies
 - System computes age from DOB and Interview Date for access to most investigators
 - System provides DOB only to Principle Investigator, hidden from all other users including DBA
 - » Selective Encryption of Genotypic Data?

Oracle World : Sept 9, 2003 : 15 :: 23



Virtual Private Database for Security

Pros:

- » Dynamically assign predicates at runtime; minimize need for complex roles and grants.
- » Assign multiple security policies to each object; stacked upon prior base policies.
- » Security policy attached to data; users cannot bypass policies embedded in applications

Cons:

- » Access rules created within stored procedures, which must be programmed and can be changed.
- » Foreign key referential integrity can be used to bypass fine-grained access policies

Oracle World : Sept 9, 2003 : 16 :: 23



Oracle Label Security: Process

Goal: Assign sensitivity labels to data for allowing selective access.

- Define **security policies** and **label components** to identify how the data needs to be secured.
 - » *Levels*: hierarchical or increasing levels of data sensitivity
 - » *Compartments*: categories for restricting data access
 - » *Groups*: capture hierarchical ownership of data
- Establish **user session labels** to define row-level security policies possible for each user, combining relevant label components.
- Oracle creates a **row label** column for each table that needs to enforce row-level security.
- **Access Mediation**: When a row is accessed Oracle checks which permissions required to access row, and what actions to perform.
- Manage Security Policies through PL/SQL Scripts and GUI-based *Oracle Policy Manager*

Oracle World : Sept 9, 2003 : 17 :: 23



PhenoDB: Using Oracle Label Security

Key Security Policies

- » Hierarchical Roles for Privileges to Clinical Studies & Instruments
- » Selective & Hierarchical Access to Data within different Project Sites

Label Components

- » *Levels*: Shareable, Internal, Confidential
- » *Compartments*: TS-Boston, TS-Utah, TS-London, TS-Toronto etc.
- » *Groups*: Project Director, Principle Investigator, Investigator, RA etc.

Combining label components to support complex security policies

- » Project Directors of TS-Boston can only set privileges for users in Boston, and access/update all levels of information.
- » Principle Investigators in TS-London can only set privileges for their own RAs, and only access/update Shareable and Internal information.
- » Investigators in TS-Utah can view sharable information from TS-Toronto

Oracle World : Sept 9, 2003 : 18 :: 23



Role of Auditing

- Minimal Auditing
 - » Capture user access
 - » Use of system privileges
 - » Changes to the database schema structure
- Critical Auditing
 - » Monitoring data change access on critical tables
- Challenges and Problems
 - » Auditing perceived to be complex to setup & use
 - » Complete Audit trails are large and difficult to interpret
 - » Auditing all tables and views affects database performance



Approach for Auditing in Oracle

- Selective and Simplified Auditing
 - » Goal: Allow high-level monitoring and audit selective details
 - » Simplify Audit trail setup to ensure it is regularly used
 - » Define critical actions to monitor that “trigger” relevant report logs
- Oracle Auditing Features
 - » **Oracle Audit** – monitoring read/write/delete access on tables
 - » **System Triggers** – monitoring start/shutdown, logon/off, creation/update to schema objects
 - » **Update, Delete, Insert Triggers** – capturing row level updates
 - » **Fine Grained Audits (FGA)** – Capturing Read Access by matching SQL queries to pre-defined predicates
 - Provided by PL/SQL package called DBMS_FGA
 - » **System Logs** – monitoring standard log files for system and structural changes



PhenoDB: Auditing for Clinical Research Database

- Monitoring Access Problems & Potential Abuse
 - » Failed logins and access with non-existent users
 - » Attempts to access database at unusual hours

- Monitoring Changes to Clinical Protocols
 - » Trigger Audit Reports for instruments created/updated

- Monitoring Data Query, Submission & Validation
 - » Fine-grained audits for SQL queries matching prior predicates e.g. specific phenotypic parameters
 - » Triggers for data submission beyond normative range of responses
 - » Triggers based on data updates for validation of clinical data

Oracle World : Sept 9, 2003 : 21 :: 23



Summary

- Distributed collaboration in clinical research settings present unique requirements & challenges for databases, particularly:
 - » Managing hierarchical roles, complex privileges & selective data access

- PhenoDB: Centralized repository to manage diverse clinical studies across multiple projects and sites, with integrated data access

- Ensuring Compliance with HIPAA Regulations
 - » Privacy Rules and Security Standards

- Oracle Security Features
 - » Selective Data Encryption
 - » Oracle Label Security
 - » Oracle Auditing

Oracle World : Sept 9, 2003 : 22 :: 23



HIPAA and Oracle Security References

1. Understanding the HIPAA Privacy Rule. *National Institutes of Health, 2003*
 - » http://privacyruleandresearch.nih.gov/pr_02.asp
2. The Final HIPAA Security Rule. *Tom Grove, Feb 2003*
 - » <http://www.hipaadvisory.com/regis/finalsecurity/summaryanalysis.htm>
3. HIPAA Auditing for Oracle Database Security. *Donald Burluson & Arup Nanda, Rampant TechPress, Sept 2003*
 - » http://www.dba-oracle.com/bp/bp_book11_audit.htm
4. Oracle Label Security. *Jim Czuprynski, Aug 2003*
 - » <http://databasejournal.com/features/oracle/article.php/3065431>
5. Introduction to Simple Oracle Auditing. *Pete Finnigan, Apr 2003*
 - » <http://www.securityfocus.com/infocus/1689>
6. The Virtual Private Database in Oracle9iR2. Understanding Oracle9i Security for Service Providers. *Oracle White Paper, Jan 2002*
 - » <http://otn.oracle.com/deploy/security/oracle9iR2/content.html>

