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

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
PhenoDB Interface: Managing Clinical Studies

Challenges for Databases in Clinical Research Settings

- **Ensuring a robust, scaleable 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?


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
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](http://www.hipaadvisory.com/regs/finalsecurity/summaryanalysis.htm)

Data Privacy and Security: Implications of HIPAA

- Authentication
- Integrity
- Authorization
- Availability
- Confidentiality
- Auditing
Data Privacy and Security: Utilizing Oracle9iR2 Features

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

PhenoDB: Oracle Privacy and Security Approaches

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

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 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**

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
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

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
HIPAA and Oracle Security References

   » http://privacyruleandresearch.nih.gov/pr_02.asp

   » http://www.hipaadvisory.com/regs/finalsecurity/summaryanalysis.htm


   » http://databasejournal.com/features/oracle/article.php/3065431

5. Introduction to Simple Oracle Auditing. Pete Finnigan, Apr 2003
   » http://www.securityfocus.com/infocus/1689

   » http://otn.oracle.com/deploy/security/oracle9iR2/content.html