

HIPAA Concerns: Implementing Tight Data Security

Chris Sherwin
Dunn Solutions Group

Business Objects

INSIGHT

AMERICAS 2006

Dunn Solutions Group

Breakout Information (Hidden Slide)

► HIPAA Concerns: Implementing Tight Data Security

- HIPAA regulations mandate that only authorized users can view medical data. This session focuses on how to implement data security for your data warehouse such that data security is seamlessly integrated into your ad hoc reporting environment. A well-implemented data security model addresses three goals: (1) security is enforced for ad hoc reporting, as well as shared corporate and private documents, (2) security has a minimal impact on query performance, and (3) the security model is easy to maintain as your user requirements change. Learn how to plan for data security when designing your data model, your universe, and enterprise security in order to achieve these three goals.

Implementing Tight Data Security

HIPAA concerns

- ▶ **Health Insurance Portability and Accountability Act of 1996**
 - HIPAA for short is a Federal Regulation impacting the distributing and sharing of individually identifiable health information (called PHI)
 - Only those with explicitly granted access are allowed to view PHI
 - Data that is not 'individually identifiable' can be more readily viewed and distributed
- ▶ **Getting the right access to the right people**
 - Giving users access to all the information they need to be best able to do their own jobs
 - Ensuring no-one has access to any PHI they are not authorized to view
- ▶ **Not Just a HIPAA problem**
 - Similar data security issues exist in any industry

Slide 3

DunnSolutionsGroup

Business Objects

Topics

- ▶ **Goals and Overview**
- ▶ **Object-Level Security**
- ▶ **Row-Level Security**
- ▶ **Data-Value (Masking) Security**
- ▶ **Summary**
- ▶ **Q&A**

Slide 4

DunnSolutionsGroup

Business Objects

Goals and Overview

Goals – what are we trying to achieve?

- ▶ **Integrated into the environment**
 - Data security enforced for adhoc reports
 - Data security enforced for shared documents
 - Data security minimizes chances of an accidental breach
- ▶ **Minimal Performance Impact**
 - Query performance similar to unsecured performance
- ▶ **Ease of Maintenance**
 - Expandable/adaptable security model
 - How hard is it to add one more User? Object? Universe?

Slide 5

DunnSolutionsGroup

Business Objects

Goals and Overview

Overview – what are we talking about?

- ▶ **What are we covering?**
 - Object-level security
 - Row-level security
 - Data-value (masking) security
- ▶ **What are we not covering?**
 - Report/category/universe security model
 - Keeping users from sharing secure data

Slide 6

DunnSolutionsGroup

Business Objects

Topics

- ▶ Goals & Overview
- ▶ Object-Level Security
- ▶ Row-Level Security
- ▶ Data-Value (Masking) Security
- ▶ Summary
- ▶ Q&A

Slide 7

DunnSolutionsGroup

Business Objects

Object-Level Security

Scenario – only some users can view the Social Security Numbers (SSN) of patients

The screenshot displays the Business Objects security configuration interface. It includes several dialog boxes and a table:

- Edit Properties of Fact Year:** Shows the 'Security Access Level' dropdown menu with options: Public, Controlled, Restricted, Confidential, and Private. The 'Public' option is selected.
- Add Restriction - New Restriction:** Shows the 'Restriction Name' as 'No SSNs' and the 'Object' as 'PatientSSN'.
- Manage Access Restrictions:** Shows a list of available restrictions and groups/users.
- Table:** A table showing the security settings for different user groups.

Name	Full Name	Object	Description	Object Level Security	Net Security
Administrators	Group		Users who can administrate this system	Private	Private
Everyone	Group		All users of this system	Public (Inherited Security)	Public

Slide 8

DunnSolutionsGroup

Business Objects

Object-Level Security

What is it?

- ▶ **Prevents users from being able to use objects**
 - By preventing access to the object, access to the data is denied
 - Two models exist
- ▶ **Security access levels**
 - Objects assigned security access level
 - Users/groups assigned security access for each universe
 - Users can only see objects for their security access and above
- ▶ **Security restricting objects**
 - Assign lists of restricted objects to each user/group

Slide 9

DunnSolutionsGroup

Business Objects

Object-Level Security

Security access levels

- ▶ **Security access level for objects**
 - Assigned access level to each objects
 - Public (least restrictive) → Private (most restrictive)
- ▶ **Security access level for users/groups**
 - Users/groups assigned security access for each universe
 - Public (least access) → Private (most access)
- ▶ **Prevents users from being able to use objects**
 - Users can only see objects for their security access and above
 - Single spectrum of restrictions per universe

Slide 10

DunnSolutionsGroup

Business Objects

Object-Level Security

Setting security access level for an object and then for a group

The screenshot shows the BusinessObjects Central Management Console interface. The main window displays a table of security settings for the 'Fiscal Year' object. The table has columns for Name, Full Name, Object, Description, and Object Level. Two rows are visible: 'Administrators' (Group) with 'Private' security level, and 'Everyone' (Group) with 'Public' security level. A dropdown menu is open for the 'Everyone' row, showing options: (Inherited Security), Public, Controlled, Restricted, Confidential, and Private. An 'Edit Properties of Fscf Year' dialog box is overlaid on the right, showing the 'Security Access Level' dropdown set to 'Public' and a 'Sort' checkbox checked. The dialog also has tabs for Definition, Properties, Advanced, and Keys, and buttons for OK, Cancel, Apply, and Help.

Name	Full Name	Object	Description	Object Level
Administrators	Group	Users who can administrate this system	Private	Private
Everyone	Group	All users of this system	Public	Public

Object-Level Security

Security access levels - meeting our goals

- ▶ **Integrated into the environment**
 - ☺ Automatically part of adhoc reports
 - ☹ Security is ignored for distributed reports
- ▶ **Minimal performance impact**
 - ☺ Zero runtime performance hit
- ▶ **Ease of maintenance**
 - ☺ Simple model minimizes chances of complexity creep
 - ☹ Difficult/impossible to give a user access to one object without others
 - ☺ Adding a new user or universe object fairly easy
 - ☹ Is all or nothing – user can see all values in field or none

Object-Level Security

Security restricting objects

- ▶ **Create lists of restricted objects**
 - As many lists as needed, each independent
- ▶ **Assign restricted lists to users/groups**
 - Assign a restriction configuration to as many users/groups as desired
 - Complexity when user belongs to multiple restricted groups

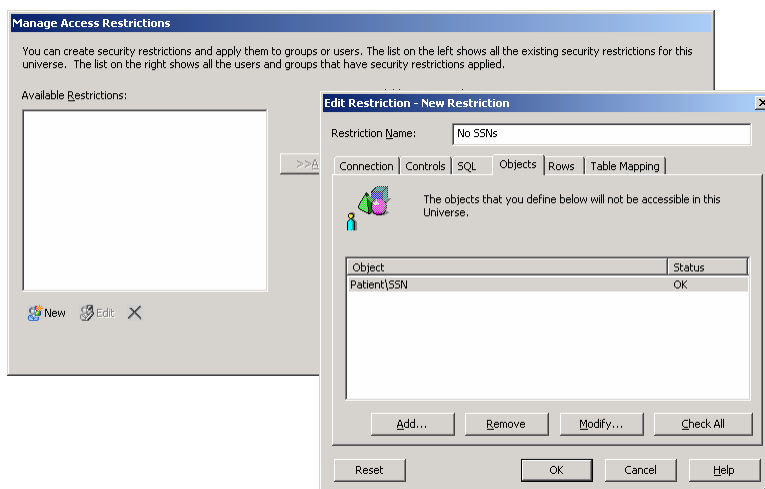
Slide 13

DunnSolutionsGroup

Business Objects

Object-Level Security

Restricting object access – creating a new restriction



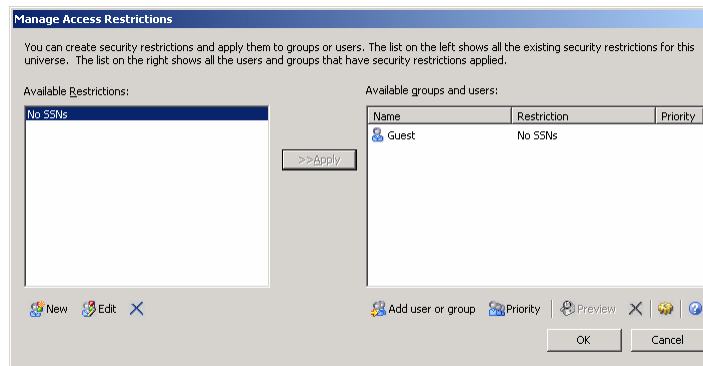
Slide 14

DunnSolutionsGroup

Business Objects

Object-Level Security

Restricting object access – applying the restriction to a group



Slide 15

DunnSolutionsGroup

Business Objects

Object-Level Security

Security restricting objects - meeting our goals

- ▶ **Integrated into the environment**
 - ☺ Automatically part of an adhoc report
 - ☹ Security is ignored for distributed reports
- ▶ **Minimal performance impact**
 - ☺ Zero runtime performance hit
- ▶ **Ease of maintenance**
 - ☺ Fully customizable object lists for each user/group
 - ☹ Memberships in multiple groups and precedence orders makes management complicated
 - ☺ Adding a new user is fairly easy
 - ☹ Adding a new object means updating security in multiple restrictions
 - ☹ Is all or nothing – user can see all values in field or none

Slide 16

DunnSolutionsGroup

Business Objects

Topics

- ▶ Goals & Overview
- ▶ Object-Level Security
- ▶ Row-Level Security
- ▶ Data-Value (Masking) Security
- ▶ Summary
- ▶ Q&A

Slide 17

DunnSolutionsGroup

Business Objects

Row-Level Security

Scenario – users can only view records in specific regions

The image displays three screenshots of the Business Objects Row-Level Security configuration interface. The first screenshot, titled "Full Restriction - New Restriction 7", shows a "Restriction Name" of "Region AA only" and a "Where Clause" of "FACT_PROCEDURES_PERFORMED.region_id = 'AA'". The second screenshot, titled "Full Restriction - Dynamic Row Restriction", shows a "Restriction Name" of "Dynamic Row Restriction" and a "Where Clause" of "FACT_PROCEDURES_PERFORMED.region_id in (select region_id from user_regions...)" and "DUP_PATIENT.region_ID in (select region_id from user_regions...)". The third screenshot, titled "New Row Restriction", shows a "Table" of "FACT_PROCEDURES_PERFORMED" and a "Where Clause" of "FACT_PROCEDURES_PERFORMED.region_id in (select region_id from user_regions where bouster = upper(Variable('USER')))".

Slide 18

DunnSolutionsGroup

Business Objects

Row-Level Security

What is it?

- ▶ **Restricting access to entire records based on security**
 - Additional where clauses are added to queries
- ▶ **Where clause tied to each table**
 - Whenever secured table is used where clause added
 - Cannot depend on other tables existing in the query

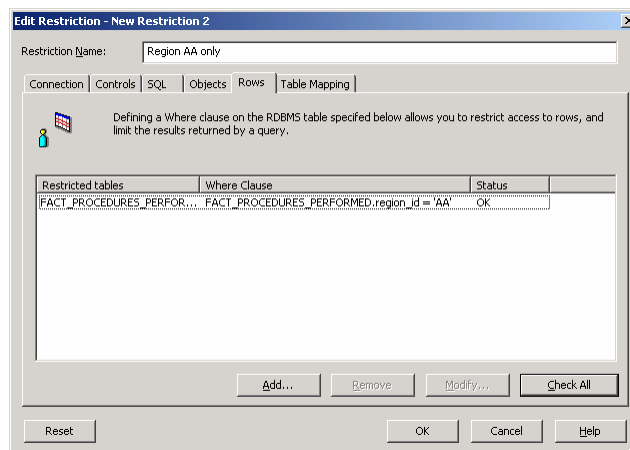
Slide 19

DunnSolutionsGroup

Business Objects

Row-Level Security

Static row restriction



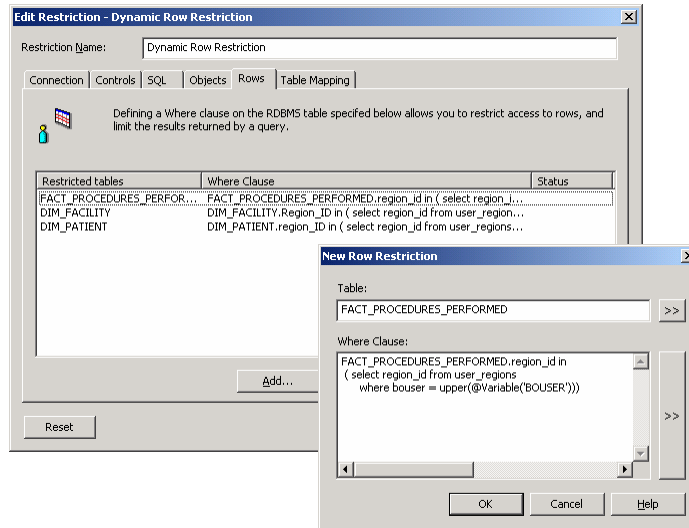
Slide 20

DunnSolutionsGroup

Business Objects

Row-Level Security

Dynamic row restriction



Slide 21

DunnSolutionsGroup

Business Objects

Row-Level Security

Meeting our goals

- ▶ **Integrated into the environment**
 - ☺ Automatically part of an adhoc report
 - ☺ Distributed reports adjusts to refreshing user
- ▶ **Minimal performance impact**
 - ☹ runtime impact depends greatly on queries used
- ▶ **Ease of maintenance**
 - ☹ Character limit (250) on row clause limits sophistication of security
 - ☹ Security clause limited to fields within secured tables
 - ☺ Adding new objects on secured tables easy
 - ☹ Difficult to maintain consistent results as user changes queries to include fewer or more secured tables.

Slide 22

DunnSolutionsGroup

Business Objects

Topics

- ▶ Goals & Overview
- ▶ Object-Level Security
- ▶ Row-Level Security
- ▶ Data-Value (Masking) Security
- ▶ Summary
- ▶ Q&A

Slide 23

DunnSolutionsGroup

Business Objects

Data-Value (Masking) Security

Scenario – users can view PHI in some regions but only demographics in others

The screenshot displays the Business Objects Data Value Masking configuration interface. It features several overlapping windows:

- Default Tables:** A window showing a list of tables with columns like 'Program_ID', 'New_Date', 'New_State', and 'New_TEND'. It includes a 'Cardinality' section and an 'Expression' field containing a complex SQL query.
- Developer - Physical Procedures:** A window showing a tree view of physical procedures, including 'NEW_SUPPLIER' and 'NEW_SUPPLIER_SUPPLEMENT'.
- SQL Statement of Test User:** A window displaying a SQL query: `select user_regions.New_ADRS = 'Y' where user_regions.New_ADRS = 'Y' and user_regions.New_State = 'NY'`.
- Table Mapping:** A window titled 'Table Mapping' showing a mapping between 'Original Table' (user_regions) and 'Replacement Table' (New_Supplier_regions).

Slide 24

DunnSolutionsGroup

Business Objects

Data-Value (Masking) Security

What is it?

▶ **Replacing**

- Data values user is not allowed to see masked with a generic value
- Allows users access to general totals where allowed, and detailed information where allowed

▶ **Two main approaches**

- Derived tables
- User-security table join

Slide 25

DunnSolutionsGroup

Business Objects

Data-Value (Masking) Security

Derived tables

▶ **Defining**

- Like a view, but defined in the universe
- Derived table definition can reference properties such as the BusinessObjects user name
- Objects are built from derived field definitions

▶ **Advantages**

- Security contained entirely in derived table definition
- Object definitions simple references to derived table fields

▶ **Disadvantages**

- Complex from clauses (entire derived table listed if even one field is referenced)
- On some databases a derived table disables the use of indexes on joined tables

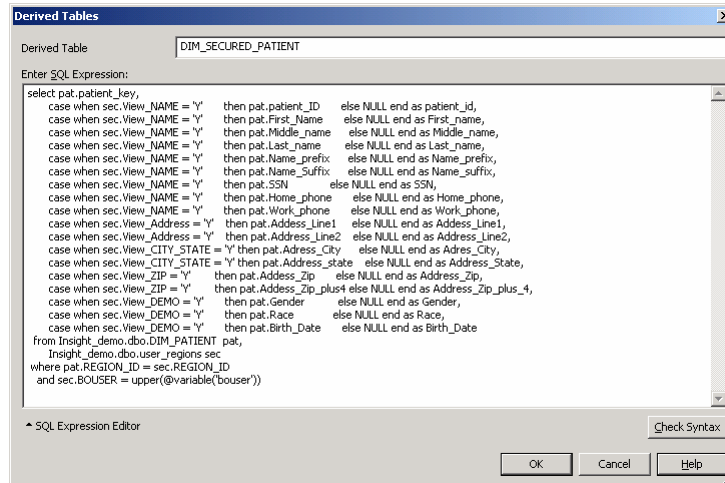
Slide 26

DunnSolutionsGroup

Business Objects

Data-Value (Masking) Security

Defining a derived table



Slide 27

DunnSolutionsGroup

Business Objects

Data-Value (Masking) Security

Meeting our goals

- ▶ **Integrated into the environment**
 - 😊 Automatically part of an adhoc report
 - 😊 Distributed reports adjusts to refreshing user
- ▶ **Minimal performance impact**
 - 😞 Disables joining Indexes on some databases
- ▶ **Ease of maintenance**
 - 😊 New objects same as unsecured
 - 😊 New users involves small configuration
 - 😞 Derived table: The derived table itself can be complicated to maintain

Slide 28

DunnSolutionsGroup

Business Objects

Data-Value (Masking) Security

Joined security table

▶ Defining

- A table defining security is directly joined
- Either a single table with a record for every user for each record (or class of records) in secured table
- Objects defined using both the data table and the security table using case type logic to determine and display either the real value or some generic 'masking' value

▶ Advantages

- Simple from clauses for queries
- All joins are table to table, field to field, so indexes should be used

▶ Disadvantages

- Object definitions are no longer simple field references

Slide 29

DunnSolutionsGroup

Business Objects

Data-Value (Masking) Security

Using joined security table

The screenshot displays the Business Objects Designer interface for a 'Physician Procedures' model. An 'Edit Join' dialog box is open, showing a join between 'Table1' (user_regions) and 'Table2' (user_regions). The join is defined with a 1:1 cardinality and the expression 'user_regions.BOUSER=upper(@variable('bouser'))'. The dialog also shows options for 'Outer join' and 'Cardinality'.

The background shows a data model with the following tables and fields:

- DIM_PHYSICIAN**: Physician_Key (N), physician_ID (C)
- DIM_PATIENT**: Patient_Key (N), Patient_ID (C), First_name (C), Middle_name (C), Last_name (C), Name_prefix (C), Name_Suffix (C), SSN (C), Home_phone (C)
- DIM_DATE**: DATE_KEY (N), Date_value (C), Year (C), Quarter (N), Month (N), Month_in_quarter (N), month_short (C), month_long (C)
- user_regions**: BOUSER (C), Region_ID (C), View_NAME (C), View_Address (C), View_CITY_STATE (C), View_ZIP (C), View_DEMO (C)

The 'PERFORMED' table is also visible in the model.

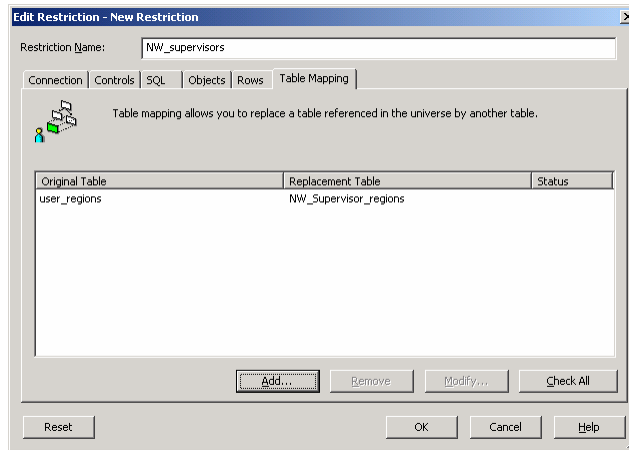
Slide 30

DunnSolutionsGroup

Business Objects

Data-Value (Masking) Security

Using joined security table - variant multiple tables



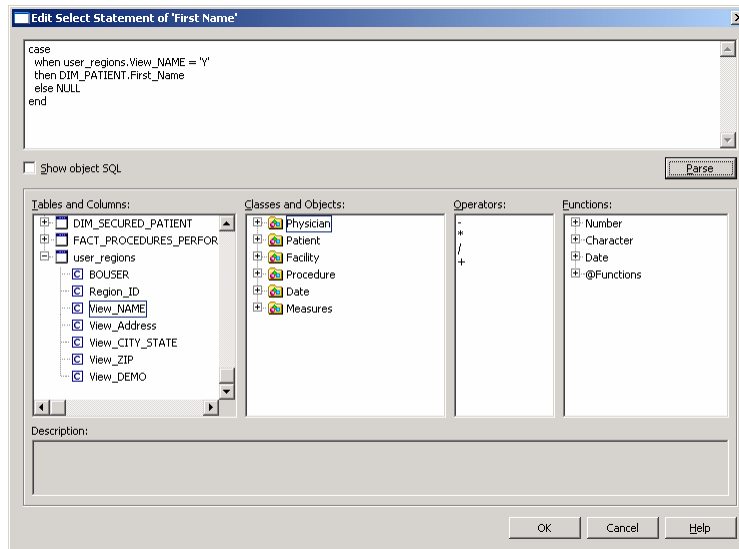
Slide 31

DunnSolutionsGroup

Business Objects

Data-Value (Masking) Security

Defining objects with joined security tables



Slide 32

DunnSolutionsGroup

Business Objects

Data-Value (Masking) Security

Meeting our goals

- ▶ **Integrated into the environment**
 - ☺ Automatically part of an adhoc report
 - ☺ Distributed reports adjusts to refreshing user
- ▶ **Minimal performance impact**
 - ☹ Indexes and direct joins minimize impact
- ▶ **Ease of maintenance**
 - ☹ New objects more complex
 - ☺ New users usually easy to add, but depends on security model
 - ☹ New universe complicated by need to create several objects

Slide 33

DunnSolutionsGroup

Business Objects

Topics

- ▶ **Goals & Overview**
- ▶ **Object-Level Security**
- ▶ **Row-Level Security**
- ▶ **Data-Value (Masking) Security**
- ▶ **Summary**
- ▶ **Q&A**

Slide 34

DunnSolutionsGroup

Business Objects

Summary

What have we talked about?

▶ **Three main techniques (plus variants)?**

- Object-level security
 - Security access levels
 - Security restricting objects
- Row-level security
 - Static row-restriction
 - Dynamic row-restriction
- Data-value (masking) security
 - Derived tables
 - Joined security table

Summary

Integration concerns?

▶ **Using security restrictions for multiple purposes**

- Object restriction, row-level restricting, table mapping
- One restriction configuration per group
- Different types of restrictions need to be maintained together

▶ **Security being defined twice**

- Configurations both in database and in the Central Management Console (CMS)
- Very easy to end up with redundant configurations
- Redundant configurations harder for maintenance

Topics

- ▶ **Goals & Overview**
- ▶ **Object-Level Security**
- ▶ **Row-Level Security**
- ▶ **Data-Value (Masking) Security**
- ▶ **Summary**
- ▶ **Q&A**

Slide 37

DunnSolutionsGroup

Business Objects

Q&A

- ▶ **Questions**
 - Call Dunn Solutions Group at 1-800-486-3866 x 108

DunnSolutionsGroup

Slide 38

DunnSolutionsGroup

Business Objects