



*Protect the privacy of confidential data in non-production environments*

IBM **Information Management** software

## IBM Optim Data Privacy Solution

---

### Highlights

---

- ***Protect the privacy of confidential data across non-production environments***
- ***Apply predefined masking techniques to speed time to delivery***
- ***Preserve the integrity of the data, while protecting privacy***
- ***Improve flexibility for masking data in existing non-production databases***
- ***Support privacy regulations and corporate governance standards***

### **Data privacy compliance — it's the law!**

Safeguarding the privacy of personally identifiable data is not just good business practice — it's the law! Companies worldwide are subject to government regulations enacted to protect confidential information from misuse. For example, the European Union has established the Personal Data Protection Directive as the framework for privacy protection governing its member countries. In Canada, organizations follow the provisions of the Personal Information Protection and Electronic Documents Act (PIPEDA), while Australian companies are subject to the Privacy Amendment Act. In the US, a number of regulations apply at the national and state levels. Similar statutes exist worldwide.

Additionally, industry coalitions are developing sector-specific governance standards. For instance, the Payment Card Industry Data Security Standard (PCI DSS), initiated by Visa® and MasterCard®, is being adopted by other

payment card companies in response to the overwhelming incidence of data theft and fraud. The Standard requires members, merchants and service providers to apply 12 security safeguards for the protection of cardholder data. In particular, PCI requirement 6.3.4 states that test databases must not contain personal account numbers (PANs) from production data.

Across industries, organizations must protect confidential employee and customer information, as well as corporate confidential data and intellectual property — no matter where it lives. More companies are gaining an understanding of the vulnerabilities across application environments. The same methods that protect data in production, such as access controls and authentication schemes, as well as network, application and database-level security, may not meet the unique requirements for protecting non-production (development, testing and training) environments.

While companies spend a great deal of time and money to secure their systems from external attacks, many do not realize that 70 percent of data breaches are from internal sources!<sup>1</sup> Examples range from employees, who misuse payment card numbers and other sensitive information, to those who save confidential data on laptops that are stolen or misappropriated. Lastly, outsourcing application development and testing activities makes it difficult to control access to sensitive data.

### **Protecting privacy in non-production environments presents challenges**

So, what makes non-production environments so vulnerable? The answer lies in understanding how non-production databases are created and used. In most cases, realistic data is required to test application functionality and to ensure accuracy and reliability.

Most often, testing environments are created by simply cloning copies of the production database. By definition, this means that sensitive information is propagated from a secure production environment to one or more vulnerable non-production environments. Do non-production environments really need to contain production data? The answer is “No.” Although using realistic data is essential for quality application testing, capabilities for “de-identifying” or masking production data offer a best practice approach for protecting privacy.

De-identifying data is the process of systematically removing, masking or transforming data elements that could be used to identify an individual. Data de-identification enables developers, testers and trainers to use realistic data and produce valid results, while still complying with privacy protection rules. Data that has been scrubbed or cleansed in such a manner is generally considered acceptable to use in non-production environments. Once the data is masked, even if it is stolen, exposed or lost, the data will be of no use to anyone.

Data masking is not simple! From a technical perspective, data masking is not a one-time process and must be appropriate for existing development, testing and training requirements. From a business perspective, a single-point solution is not the most cost-effective approach. The ideal solution must support data privacy compliance across applications, databases, operating systems and hardware platforms.

### **Protect privacy and reduce disclosure risk**

As a recognized best practice, de-identifying data provides the most effective way to protect privacy and support compliance initiatives. The IBM® Optim™ Data Privacy Solution provides comprehensive capabilities for de-identifying application data that can be used effectively across non-

production environments. You can take the necessary steps to protect privacy, while still providing the necessary “realistic” data for use in development, testing, training or other legitimate business purposes.

Optim’s scalable data masking techniques can be deployed across applications, databases, operating systems and hardware platforms to meet your current and future needs. De-identified data is safe and valid to use in non-production environments. The masked test data still makes sense to developers, testers and trainers and produces accurate, reliable results, but is worthless to thieves and hackers. When you use Optim to de-identify confidential test data, you minimize disclosure risks — and force thieves to turn elsewhere.

### **Implement proven data masking techniques**

Using Optim, developers and testers can apply a variety of proven data transformation techniques to substitute confidential data with contextually accurate, but fictionalized data to produce valid results. With support for the leading database management systems, Optim also provides federated access capabilities that allow you to extract and mask appropriate data from multiple production data sources in a single process.

In addition, Optim's "mask-in-place" capability allows you to mask data that was extracted using third-party tools or data that already resides in other non-production environments. Organizations that have data in place for testing, or that use backup type facilities to create those test databases can benefit from Optim's "mask-in-place" capabilities. Using Optim to mask data directly at the source eliminates the need to move the data for additional processing and still preserves the referential integrity of the data.

Optim's application-aware masking capabilities help ensure that masked data, like names and street addresses, resembles the look and feel of the original information. Optim preserves the integrity of the data and produces consistent and valid results that reflect the application logic. For example, surnames can be replaced with random surnames, not with meaningless text strings.

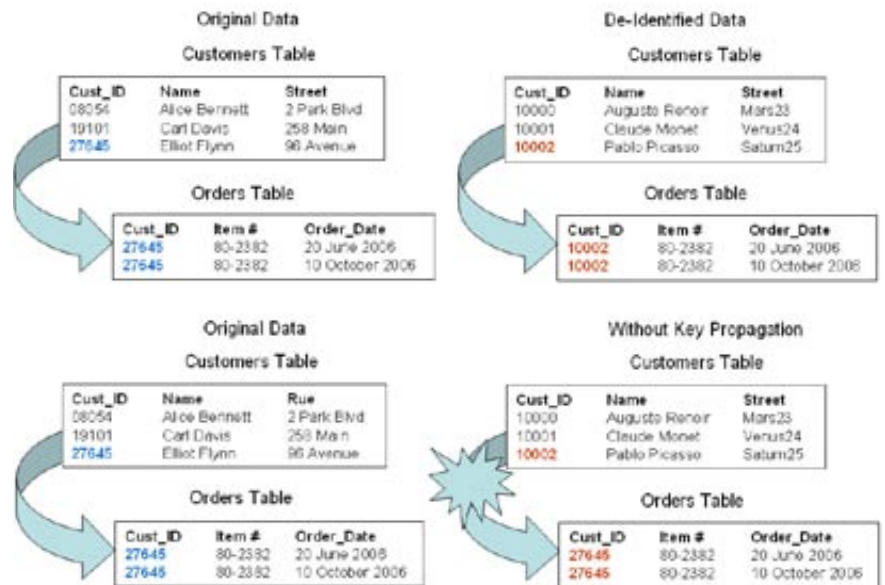
Context-aware, prepackaged data masking routines make it easy to de-identify many types of sensitive information, such as birth dates, bank account numbers, national identifiers (like Canada's Social Insurance numbers or Italy's Codice Fiscale), benefits information, health insurance identification numbers and so on. Some examples of Optim's masking techniques include substrings, arithmetic expressions, random or sequential number generation, date aging and concatenation.

Optim's Transformation Library™ routines allow for accurately masking complex data elements, such as Social Security numbers, credit card numbers and e-mail addresses. Built-in lookup tables support masking names and addresses. You can also incorporate site-specific data transformation routines that integrate processing logic from multiple related applications and databases and provide greater flexibility and creativity in supporting even the most complex data masking requirements.

Each of the methods described so far is effective for masking data to safeguard confidentiality. However, with relational database applications, there is an added complication. Specifically, you need the capability to propagate a masked data element to all related tables in the database to maintain the referential

integrity. For example, if a masked data element, such as a telephone number, is a primary or foreign key in a database table relationship, then this newly masked data value must be propagated to all related tables in the database or across data sources.

Key propagation helps preserve the referential integrity of the transformed data across applications, databases and operating environments. Without key propagation, the relationships between parent and child tables would be severed, causing the test data to be inaccurate. Consequently, application testing will produce unreliable results. Optim's persistent masking capabilities propagate masked replacement values consistently and accurately across multiple data sources to generate valid test results.



Optim offers a variety of data masking techniques to protect the confidentiality of private information.

## Support your data privacy and security initiatives

Optim provides a single, scalable data privacy solution with flexible capabilities that can be easily adapted to your current and future requirements. Implementing Optim helps you comply with data privacy regulations and protect the confidentiality of sensitive information across your enterprise. You also benefit from knowing that Optim supports all leading enterprise databases and operating systems, including IBM DB2®, Oracle®, Sybase®, Microsoft® SQL Server®, IBM Informix®, IBM IMS™, IBM VSAM®, Teradata®, Adabas®, Microsoft Windows®, UNIX®, Linux® and IBM z/OS®. In addition to providing data management support for all custom and packaged applications, Optim also supports the key ERP and CRM applications in use today: SAP® Applications, Oracle® E-Business Suite, PeopleSoft® Enterprise, JD Edwards® EnterpriseOne, Siebel® and Amdocs® CRM.

## About IBM Optim Integrated Data Management Solutions

IBM Optim Integrated Data Management Solutions offer proven, integrated capabilities to manage enterprise application data from requirements to retirement. With Optim, teams can share data artifacts (like models, policies and metadata) to align data management with business goals and improve collaboration. Today, organizations of all types leverage Optim to improve performance, streamline database administration, speed application development, and enable effective governance. Optim delivers better business outcomes, at lower cost, with less risk, while providing capabilities that scale across enterprise applications, databases and platforms.

### For more information

To learn more about IBM Optim Integrated Data Management Solutions, contact your IBM sales representative or visit: [www.ibm.com/software/data/optim-solutions/](http://www.ibm.com/software/data/optim-solutions/).



© Copyright IBM Corporation 2008

IBM Software Group  
111 Campus Drive  
Princeton, NJ 08540-6400  
U.S.A.  
[www.optimsolution.com](http://www.optimsolution.com)

Produced in the United States of America  
12-08  
All Rights Reserved

<sup>1</sup> Richard Mogul, "Danger Within – Protecting your Company from Internal Security Attacks," *Gartner*, August 2002.

DB2, IBM, the IBM logo, IMS, Informix, Optim, VSAM and z/OS are trademarks or registered trademarks of the IBM Corporation in the United States, other countries or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. UNIX is a registered trademark of The Open Group in the United States and other countries. Windows and SQL Server are registered trademarks of Microsoft Corporation in the United States and other countries. All other company or product names are trademarks or registered trademarks of their respective owners.

References in this publication to IBM products, programs or services do not imply that IBM intends to make them available in all countries in which IBM operates or does business.

Each IBM customer is responsible for ensuring its own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.