**IBM DB2 Anonymous Resolution Whitepaper**
May 2005

DB2® Information Management Software

# IBM DB2 Anonymous Resolution: Knowledge discovery without knowledge disclosure

*Andrew Friedrich*
*Worldwide Product Marketing Manager*
*IBM DB2 Entity Analytic Solutions*

Contents

## Executive Summary

Sharing information about identities (e.g., individuals, employees or customers) is an effective tool for discovering knowledge and increasing the effectiveness and economy of public and private programs and initiatives. Responsible managed, information sharing can help:

- Recognize and eliminate fraud;
- Identify beneficiaries;
- Reveal business opportunities; and
- Provide a powerful enhancement to fighting the war on terror

> *"The 9/11 Commission has made observations regarding information sharing, and recommended procedures to provide incentives for sharing and creating a 'trusted information network.'"*
>
> "Testimony before the Committee on Government Reform, House of Representatives", Government Accountability Office, August 3, 2004

With the benefits of such collaboration comes a great responsibility to the individuals whose information is being shared. The public must know for certain that their privacy is being protected and that the information they have entrusted to their governments, or the companies with whom they do business, is not being abused:

> *"It's a basic principle of data protection that personal information that we give for one purpose should not then be used for another purpose without our consent. This is particularly important since we often have no choice about giving government the information in the first place – on tax returns, to receive benefits, to drive, or to obtain a passport."*
>
> "Privacy and Data Sharing - Liberty Response to PIU Report", Liberty, April 11, 2002

Intended or unintended, organizations who violate this trust risk exposure to legal action as well as severe damage to their reputation and brand. The purpose of this paper is to discuss the utility of IBM's DB2® Anonymous Resolution software, a new solution for de-identifying personally identifiable information assets.

This document will examine the potential of this technological breakthrough to reduce trust-based risks and change the way organizations reach a harmonious balance between consumer privacy and information sharing.

**Key Benefits of DB2 Anonymous Resolution**

- Enable the exchange and correlation of information where it has not been possible in the past.
- Enhance protections against unintended information disclosure.
- Enable multi-party, multi-system discovery without information disclosure.
- Protect anonymity of sensitive data.
- Prevent data re-purposing.
- Permit data to remain in the control of the data owner.
- Protect the privacy of customers and employees.
- Reduce exposure to privacy violations, both regulatory and corporate-based.
- Uncover the true customer value and/or risk of a merger or acquisition.
- Achieve a balance between homeland security missions and privacy interests.
- Enable safe & selective data sharing.

## Business Challenge

Collaborative sharing of information can raise significant issues, regardless of the application. Often legal, reputational, privacy, and security ramifications present such large barriers that the risk associated with multiparty information sharing initiatives often outweighs the benefit.

### Consumer Privacy

Under Section 314(b) of the USA PATRIOT Act FSP's (Financial Service Providers) are permitted to share information with one another to identify and report activities to the federal government that may involve money laundering or terrorist activity. Although many FSP's have gone through the notice/certification process, most are apprehensive about actually participating in such collaboration based on even the slightest possibility of consumer privacy and civil liberty violations that could result from information being unintentionally exposed or re-used for purposes beyond its stated intent.

### Competitive Intelligence

Companies wanting to share client lists with channel partners and alliances for joint sales/marketing campaigns or acquisition managers using client list cross-reference in their due-diligence process to gauge customer overlap and risk potential face the duel threats of consumer privacy exposures and revealing sensitive commercial intelligence to competitors.

### Criminal and Intelligence Investigations

Depending on the nature of the request, law enforcement and intelligence queries of commercial data can expose and tip off subjects-of-interest. In addition, governments are reluctant to share sensitive data with the private sector for fear of unintentionally disclosing their objectives and thereby compromising their missions.

**Customer Pain Points**

- Striking a balance between the demands of sharing information (for critical applications, e.g., Homeland Security), and the personal privacy of individuals whose personally identifiable information (PII) is being shared.
- Finding solutions that do not to violate host country privacy laws in order to conduct business with other countries (e.g., European or Asian countries sharing w/ the United States).
- Legal and cultural privacy barriers that prevent multinational corporations from sharing information across their own organizations.
- Re-assuring individuals that data gathered for one purpose is not being re-purposed for other activities.
- Not violating the privacy of individuals while offering practical uses for sharing their PII (e.g., PII sharing for improved clinical research, enhancing effectiveness of benefits administration, or stepping up anti fraud efforts).

Although it is easy to see the many upsides of information exchange, it is hard to get past the potential downsides. Most organizations have adopted a "better safe than sorry" attitude, avoiding information sharing initiatives altogether.

To overcome this barrier, central challenges must be resolved: How can businesses, governments, and countries effectively exchange knowledge without handing over their data ownership and control of disclosure? How can they secure information in the exchange process to reduce the possibility of revealing sensitive details and thus compromise  the security and privacy of the information they have been entrusted to protect?  In other words, how can they achieve knowledge discovery without having to relinquish or discover knowledge?

## Solution Description

At the Las Vegas, Nevada headquarters of IBM's Entity Analytic Solutions group, not far from the California high desert where in 1947 Chuck Yeager challenged the naysayers and broke the sound barrier, the anonymous data sharing barrier has been shattered. IBM's DB2 Anonymous Resolution software enables multiple organizations to share and compare proprietary information assets in a de-identified format that allows the original data holders to maintain control over the flow of what information is revealed and what information is concealed.

### Extending the Utility of Existing One-Way Hashing

For years, cryptologists have used one-way hash techniques to accomplish various security functions, such as digital signatures which can be used to ensure that a document has not been modified. A one way hash is basically an algorithm that converts input text data into fixed strings of alphanumeric characters.

| Input Text | Hashed Value |
|---|---|
| Dave Travars | h8Z93c7olgwILAAY2uM8 |

Conceptually speaking this capability would seem a natural fit for two organizations wishing to create a more secure environment for data sharing. Organization A, and Organization B, would simply one way hash their clear text identity information, share and then compare for common strings of alphanumeric characters. Provided that the same hash algorithm is in use at both sites and the original input text information being sought is “identical” prior to being one way hashed this approach could work, it is however very unlikely given the inconsistencies and irregularities plaguing most identity information stores that would seriously degrade any insight gleaned from the process.

Using a standard hashing process, if anything changes with the input—even if one character or extra space is added—the hashed output will be expressed by an entirely different hash value, this is called an avalanche effect[1].

[1] Even a slight change in an input string should cause the hash value to change drastically. Even if 1 bit is flipped in the input string, at least half of the bits in the hash value will flip as a result. This is called an avalanche effect. - http://www.aspencrypt.com/crypto101_hash.html

In our example three records containing transposition and name variations of the same individual  have been hashed; in this case Dave Travers, David P. Traverse and Dave P Traver:

| **Input Text Record** | **One Way Hashed Value** |
|---|---|
| *Record 1* | |
| Dave Travers | h8Z93c7olgwiHCDP2uM8 |
| PPN# 786786543 | nZsLGNd3HdsQRpnLONc4 |
| SSN# 027869675 | tK8u891GbO6/3DJ1huf6 |
| *Record 2* | |
| David P. Traverse | ugis8PSaQkHhCk09IxrU |
| 1 Bourne St | sZw37siaebQ3/jSPXaos |
| Clinton MA, 01510 | h1n8O1GbO6/3D76QbFTI |
| *Record 3* | |
| Dave P. Traver | cxke9JSfLoPeRuW4BcmZ |
| TEL# 5014274475 | cdi5Rr1ElDE187KLueVDz |
| EIN# 896756453 | UI7/sdLE87/sSFE4G97P |

Although the variations in first and last name are slight the hashed values are completely different and thus recognized as three distinct identities with three hashed values. If the objective of sharing these records was to recognize duplicate customers between two data sets the resulting counts would be inaccurate.  It is important to state that the inability of one way hashing to resolve identity does not reflect a problem with one way hashing whose primary function is data de-identification, rather it recognizes the limitation of hashing alone to facilitate true knowledge discovery from an information sharing exercise

DB2 Anonymous Resolution's breakthrough is its ability to correlate identity data within a hashed data set despite inconsistencies in how identities are expressed and poor data quality. Leveraging the IBM DB2 Relationship Resolution breakthrough context-accumulating techniques (patent-pending), pre-processing techniques are applied before the one-way hash is applied.  As a result, AR achieves fuzzy-like matching properties, including the ability to recognize ambiguities, misspellings, or partial records within a data set and resolve identities across all attributes to produce the higher levels of information accuracy. In addition, AR can detect non-obvious relationships between individuals inside of the same anonymized data space.

## Anonymous Resolution Applications

DB2 Anonymous Resolution will benefit any organization that stands to gain from collaborative information sharing activities, but has been unwilling to risk the perceived exposure that has always accompanied such processes. The following applications represent a sample of the potential of this technology.

### Financial Services

Anonymous Resolution can be used to anonymize customer data to facilitate more secure cooperative data sharing (or "co-opetition", as it is referred to in the industry) between partners for joint marketing campaigns, or as a precursor to a merger or acquisition to gauge customer overlap, or to vet and identify potential risks before an acquisition takes place without the need for either party to relinquish control of their customer lists.

FSP's seeking stronger privacy and security protections surrounding multi-party information sharing under section 314 of the Patriot Act can deploy Anonymous Resolution across multiple locations to de-identify customer data sets before information sharing occurs. A central “Resolver” (in this application scenario, it could reside with a non-profit association) would resolve the multiple anonymized data sets producing alerts based on matches and relationships.

Anonymized data can help address reputational and regulatory issues associated with financial service providers sharing customer records during database marketing enhancement processes (“appends”), fraud specific collaborations with affiliates, or where required with the federal government (in a manner not requiring the implementation of Section 215 of the US PATRIOT Act).

### United States and the European Union

The U.S. and the EU have reached an agreement that requires the transmission of EU airline passenger name records (PNR) data to U.S. authorities to detect and prevent potential terrorist threats. To date, this agreement has been somewhat controversial, as EU privacy advocates have claimed that transmission of such PNR data contravenes EU privacy laws.

European air carriers could use Anonymous Resolution to anonymize and transfer passenger manifest data to a trusted third party.

> *“By securely anonymizing personal data before it is processed by an intermediary, relevant data about suspected terrorists could be shared while fully complying with the strict privacy protections of the EU Directive on data protection.”*
>
> “Anonymization, Data Matching and Privacy: A Case Study,” Steptoe and Johnson - Stewart Baker, Kees Kuilwijk, Winnie Chang, Daniel Mah, December 2003

Deidentified PNR could go a long way towards addressing EU privacy concerns and still provide the U.S. with the insight necessary to meet security requirements.

### Health Care

The accuracy of records-based medical research expands as the economy of available records expands, as patterns are more likely to be statistically significant across larger populations. HIPAA privacy rules have however created significant barriers to aggregation of identity information into a single database[2]. Using DB2 Anonymous Resolution, researchers could anonymize personal health information to enable robust medical research—including analysis and sharing of patient data, while reducing the possibilities of HIPAA or related privacy exposures.

Anonymized patient data for statistical analysis allows analysts to share and analyze the data without having to see personal identifiers of the patient by de-identifying all personal identifiers within data sets. Anonymous Resolution is also applicable within non-HIPAA-regulated health organizations such as the CDC (Center for Disease Control) and NIH (the National Institute of Health). AR enables them to gather anonymized data for insights into public health patterns while remaining consistent with privacy protections. Resolved and correlated anonymous datasets could also help reduce the common problem of double-counting in records-based research and clinical drug trials, and enable an early warning system for medical researchers to recognize emerging trends, outbreaks, or concentrated occurrences of medical conditions—without having access to the personally identifiable information of the patient populations on which is the discoveries are based.

[2] Violating the HIPAA privacy rules, 45 C.F.R. § 164.512(i) & § 164.514(c), -Research records to be shared where they are “de-identified” up to the standards of Section 164. - Where the sharing of records involves only a “limited data set.” To qualify as a limited data set, “direct identifiers” such as name and SSNs must be eliminated.

### Law Enforcement

The USA PATRIOT Act requires sharing of intelligence between law enforcement agencies (federal to state and local) and between and among law enforcement and intelligence communities. Red flags have been raised by citizens advocacy groups fearful about the nature and type of the data being shared, as well as its security and potential for abuse. Using Anonymous Resolution, local and state law enforcement agencies can de-identify sensitive data elements before collaboration occurs. Information in an anonymized form puts the control of knowledge discovery in the hands of the data owner, significantly reducing the risk of data being revealed or misused for any purpose beyond its stated law enforcement mission.

### Service Bureaus and GSI's (Global System Integrators)

GSI's and Service Bureaus are well situated to position themselves as the trusted third party in the Anonymous Resolution value chain to facilitate certain high risk collaboration efforts. These entities are more likely to have in place the expertise and security necessary to facilitate secure third party resolution of anonymized data sets.  Service Bureaus in particular already act as outsourcers to manage the database marketing efforts of Fortune 500 clients. Their large data center's, well established customer relationships and experience in dealing with massive amounts of information make them natural fits to intermediate collaborative efforts. The sharing parties would anonymize their data sets and provide them to the trusted third party, who would resolve the data and, depending on the mission, communicate the resulting matches or alerts back to the original data holders.

### Federal Government

Anonymized data sets will increase privacy and security controls surrounding government data sharing. For example, using Anonymous Resolution to de-identify federal watch lists allows government agencies searching for money laundering or national security threats to share data from their own secure locations with financial service providers such as:

- Banks and trust companies
- Savings associations
- Credit unions
- Securities brokers and dealers
- Futures merchants and brokers

Without exposing sensitive watch lists attributes. Additionally, the risk of compromising an investigation due to the sensitive detail contained in a federal government query on outside data source is dramatically reduced when clear text has been anonymized.

Government organizations that share the same mission—for example, social services, health or retirement benefits—can de-identify and resolve shared datasets to recognize duplicate identity information to avoid double-counting, overpayments, and other errors when processing benefits. Anonymous Resolution can facilitate responsible information sharing across multiple inter-government organizations with the same assignment to better coordinate efforts; for instance, national security and local/state law enforcement to determine if their watch lists include duplicate suspects, or within a single organization where data can be selectively revealed based on levels of clearance and the "need-to-know or share."

### ISP's (Internet Service Providers)

Legislation such as the USA PATRIOT Act and the Cyber-Security Enhancement Act (CSEA) have made it far easier for government agencies to obtain access to individuals' private electronic information in specific circumstances and under defined procedures (e.g. e-mail, voice mail, phone records, internet transactions, and chat-room transcripts). ISP's are the keepers of volumes of such data and find themselves caught between the requests of the federal government and their own corporate privacy. With Anonymous Resolution, ISP's will be able to anonymize "resolve to" identity information related to customers, allowing them to meet the national security demands of the federal government while remaining consistent with their own privacy governance guidelines and their responsibility to the privacy of their user base.

## Inner Workings

There are four main components to the DB2 Anonymous Resolution solution:

1.) "Anonymous Resolution Console" manages Anonymous Resolution configuration and alerts

2) "Anonymous Resolution Pre-Processor" performs standardization and normalization of the data elements before information is hashed

3) "Anonymous Resolution Anonymizer" hashes information into random character strings

4) "Anonymous Resolution Resolver" performs Anonymous Identity, Relationship Resolution and generates alerts

### 1) DB2 Anonymous Resolution "Console"

The Anonymous Resolution "Console" provides a graphical user interface to manage Anonymous Resolution configurations and view alerts. The "Resolver" site sets the configuration, including codes to identify data source information for "Anonymizer" site and data source, data attributes expected in each incoming anonymized data set, resolution scenarios, and alert conditions. Once set, the "Resolver" site exports a configuration file used by each "Anonymizer" site in the standardization, cleansing, and normalization process. The anonymized data records are optimized consistently for "Resolver" processing.

### 2) DB2 Anonymous Resolution "Pre-Processing"

IBM's proprietary algorithms perform a sophisticated pre-processing methodology to datasets prior to the anonymization process, including:

- Name standardization: determines and applies root names (e.g., Rob, Bob, Bobby equate to Robert).
- Address verification and correction: compares, verifies, and corrects addresses with U.S. and international address databases.
- Normalization: applies data-driven rules to addresses, phone numbers, date of birth, social security numbers, and other significant attributes in preparation for hashing.

### 3) DB2 Anonymous Resolution "Anonymizer"

The "Anonymizer" then processes the data through a one-way hash function, which applies an industry-standard cryptographic, pre-image resistant hash to de-identify the data by transforming the values into a form that is computationally and mathematically irreversible. A one-way hash essentially turns names, addresses, and other input text information into strings of alphanumeric characters that are mathematically impossible to convert back to their original form.

| **Input Text** | **Hashed Value** |
|---|---|
| PPN# 8769882727 | h8Z93c7olgwiHCDP2uM8 |

The resulting de-identified data sets are sent to a "Resolver" site where Identity and Relationship Resolution are performed. Alerts are then generated based on matches and relationships detected within the hashed data set.  The transformed, anonymized data can now be shared with other parties, while the actual data remains safe in the owner's database or repository

Different anonymization missions may in fact require different types of hashes.  For example, a government agency sharing and resolving anonymized individual data sets across international boundaries may have different hash requirements than two domestic banks sharing and comparing anonymized customer lists in the same city. DB2 Anonymous Resolution is hash-agnostic and can utilize a variety of industry standard one-way hashes based on the needs of the customer.

### 4) DB2 Anonymous Resolution "Resolver"

The "Resolver" receives the anonymized (hashed) data from multiple sources and performs Anonymous Resolution by identifying matches in the anonymized content database. The "Resolver" generates alerts that indicate the discovered matches and relationships, which are passed along to the data owners, as appropriate. The "Resolver" can concurrently process hashed data from countless "Anonymizers". The Resolver leverages two proprietary IBM technologies, DB2 Identity Resolution and DB2 Relationship Resolution.

#### Anonymous Identity Resolution

This Anonymous Identity Resolution process determines whether multiple records that appear to describe different individuals or organizations, even with different identity variations and attributes, are actually records for a single resolved identity. Once the process has determined that two or more identities are the same, the multiple records are conjoined by sharing a common persistent key. The resolved identity data is presented in a comprehensive, unified view that maintains all of the data's original attributes, such as information about the individual or organization from prior records—even identifying the source systems that provided the original data.

#### Anonymous Relationship Resolution

After Anonymous Identity Resolution, relationships are discovered, allowing users to identify non-obvious relationships across anonymized data sets. The software recognizes commonalities between unique identities such as persons sharing the same address, cell phone number, or bank accounts. When a high risk relationship has been uncovered based on user parameters set in the console, Anonymous Resolution's link analysis instantly triggers an alert that flags the anonymized record in question. Users are only presented with pointers to record holders, never any personally identifiable identifiers.

## Operational Process

A basic DB2 Anonymous Resolution operational process for a health care study would look like this:

1) Original Input Text Source Data:
   Relevant databases (e.g., prescription records, admittance records, outcome records, medical tests, etc.) containing such information as names, addresses, phone numbers, birth dates and Social Security numbers are identified.

2) XML Formatting:
   The source data is formatted into an industry standard XML record with prescribed field tags.

3) Pre-Processing Applied:
   Data is pre-processed in a way necessary to perform identity resolution. For instance, the names Bob, Rob, Robbie, or Bobby are treated as functionally equivalent to Robert.

4) Domain Specific Salt Value Added:
   A secret "SALT" value[3] is added to enhance security and prevent a dictionary attack against the anonymized data set.

5) One-way Hash Code Applied:
   Using the "Anonymizer", information is scrambled and compressed into a unique hash value. Thereafter, these records are only of use to the party with the Resolver.

[3] (n.) (1) A method used to break security systems, specifically password-based security systems, in which the attacker systematically tests all possible passwords beginning with words that have a higher possibility of being used, such as names and places. The word "dictionary" refers to the attacker exhausting all of the words in a dictionary in an attempt to discover the password. Dictionary attacks are typically done with software instead of an individual manually trying each password. http://www.webopedia.com/TERM/D/dictionary_attack.html

6) Resolver Performs - Anonymous Identity Resolution:
Using the "Resolver", anonymous Identity Resolution is performed to correlate the anonymized data with previously received data. Matches are produced and alerts are generated.

7) Resolver Performs - Anonymous Relationship Resolution:
Once identities have been resolved, the "resolver" performs relationship resolution to uncover non-obvious relationships.

8) Suspect Alert and Notification Generated:
If a match is found between records, the trusted "Resolver" party (often a third party) sends an encrypted message, based on the configuration rules.

9.) Pointers To Secure Source Record
Once a match is detected and an alert generated, the parties sharing de-identified information receive a pointer back to the original input text record housed in the original source database. Data owners who control the source system ultimately determine whether or not to disclose flagged records.

### Salt Values Enhance Security by Providing an Irreversible Digital Signature

IBM uses "salt values" in the anonymization process to reduce the advantage an attacker might otherwise have in trying to perform dictionary attacks on the hashed values. A salt value is a randomly generated secret key shared by all Anonymous Resolution "Anonymizers" providing data to the same "Resolver". The "Anonymizer" appends these random keys to the original plain text before generating hashes. The result is that each record contains a digital signature that adds an additional layer of security to the hashed value. All parties running the "Anonymizer" who wish to compare data anonymously must use the same salt value. The party running the "Resolver" is not provided the salt value. The salt value provides an additional barrier to a dictionary attack against the anonymized data and must be kept secret among the "Anonymizer" parties.

## Deployment Considerations

### Single Organization Deployment

DB2 Anonymous Resolution components can be deployed to facilitate information sharing across a single organization, for example a multinational corporation sharing information across geographic boundaries, or a government organization resolving and sharing sensitive data sets within their own systems but across departments and individuals with different levels of security clearance.

### Multi Organization Deployment

DB2 Anonymous Resolution can also be deployed across multiple organizations. In this deployment scenario, each site would run its own "Anonymizer" to de-identify information sets which would then be delivered to a central location running a "Resolver". The Resolver would resolve anonymized data to generate alerts and pointers to be used for subsequent knowledge discovery.

### Trusted Third Parties to Overcome Cultural Barriers

Despite Anonymous Resolution's ability to anonymize data and prevent re-identification, some data owners may be sceptical of relying solely on technology to guarantee the security of their information. This may be especially true in a case involving data sharing between competitors or data sharing between countries whose geopolitical interests may not be fully in alignment.

> *"We all have an inherent tendency to hoard information, to protect it, and to guard its use. It is human nature, especially in today's information-centered society."*
>
> "Overcoming Information Sharing Obstacles and Complexity", The Police Chief, November 2003

In such cases, a trusted third party (potentially a Global System Integrator or Service Bureau) can facilitate the Anonymous Resolution process and provide an additional layer of protection during collaborative information sharing. The primary function of this trusted third party would be to provide a secure, neutral location to resolve anonymized data, and communicate hits or matches produced as a result of this comparison. Privacy is enhanced because the original holders of the information continue to own and hold their source data and can operate as gatekeepers on a "need-to-share" basis regarding requests for information as made discoverable through the use of the anonymous resolution process.

### Security, Auditability, and Control

IBM DB2 Anonymous Resolution uses the security and auditability features of the host infrastructure including hardware, middleware and database engines. Customers are responsible for determining the legal basis on which they can make a data transfer using this anonymization scheme.  Customers are also responsible for the evaluation, selection, and implementation of security features, administrative procedures, and appropriate controls in application systems and communication facilities.

## Conclusion

Just as breaking the sound barrier opened the door to the creation of a whole new breed of supersonic jets, IBM's patent-pending DB2 Anonymous Resolution technology promises to do the same for collaborative information sharing initiatives.  Anonymized information assets will help organizations, both public and private, to:

- Meet the demands of secure information sharing in a privacy-enhancing manner in such areas as medical studies, law enforcement, cooperative marketing, anti fraud and watch list processing
- Overcome geographic, legal and cultural barriers that prevent information sharing due to privacy issues

DB2 Anonymous Resolution also provides the framework necessary to help:

- Protect the privacy of personally identifiable information
- Significantly reduce the risk of unintended disclosure of an organization's sensitive information
- Reduce the risk associated with data being repurposed for use in non-permissible missions

The ability to compare and correlate multiparty information anonymously, sharing only the information that is pertinent to a specific objective, holds with it the potential to vastly accelerate and shift the entire knowledge discovery process. Responsibly deployed, this anonymization technology makes possible new levels and applications of information sharing while helping address privacy and security issues.

## Contact Information

Kevin Painter, Director of EAS Sales
(702)853-4816 • (217)725-5414 (cell) • klpaint@us.ibm.com

Rakesh Goenka, Program Director of EAS Marketing
(702)853-4818) • (416)518-2954) • goenka@ca.ibm.com

Andrew Friedrich, Worldwide EAS Market Manager
(702)853-4802) • (501)247-4263) • afriedri@us.ibm.com

John Bliss, Privacy Strategist
(702)851-4683) • jblisslv@us.ibm.com

## Additional Information

For the latest information about our products and services, see the following website: **www.ibm.com**/db2/eas/

IBM (United States of America)
Entity Analytic Solutions
6600 Bermuda Rd, Suite A
Las Vegas, Nevada
United States of America, 89119

Printed in the United States of America
05-05

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

♻ Printed in the United States of America on recycled paper containing 10% recovered post-consumer fiber.

IBM's customers are responsible for ensuring their own compliance with relevant laws and regulations. It is a customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of laws and regulations that may affect a customer's business and any actions required to comply with such laws. IBM does not provide legal, accounting or audit advice or represent or warrant that its services or products will ensure that a customer is in compliance with any law.