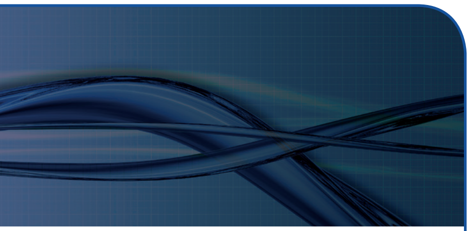


PARAT Classic

De-identification and Masking Solutions for Health Data

Privacy Analytics' software and expertise combine to offer a unique suite of products and services to de-identify, quantify, assess and manage re-identification risks when disclosing health data for secondary purposes. Using peer-reviewed metrics and de-identification algorithms created by CEO, Dr. Khaled El Emam and his team, our solutions, which are compatible with HIPAA and other international standards allow secondary users of health information to protect and share multiple data sets in support of cross-sectional, longitudinal, and geospatial analysis. Privacy Analytics works with some of the largest research organizations, pharmaceutical, healthcare , medical device and insurance providers in North America. Privacy Analytics solutions result in high quality de-identified data suitable for complex analytics while still providing strong privacy safeguards against unwanted disclosures. PARAT is a proven technology that has been used to de-identify more than 100 million records.

"We are in a unique position to give our clients the ability to cost-effectively execute big data analytics on their databases, share that data with the confidence that personal privacy is respected, and still provide the highest quality data needed by complex business intelligence tools," says Dr. Khaled El Emam, founder and CEO of Privacy Analytics. "In effect, we have democratized valuable customer or patient data for many other uses."

PRIVACY
ANALYTICS
Nothing Personal

800 King Edward Drive, Suite 3042
Ottawa, Ontario, Canada K1N 6N5

www.privacyanalytics.ca
613.369.4313
info@privacyanalytics.ca

PARAT De-Identification Software

The Privacy Analytics Risk Assessment Tool (PARAT) optimally de-identifies information to protect individual privacy while retaining the data's value.

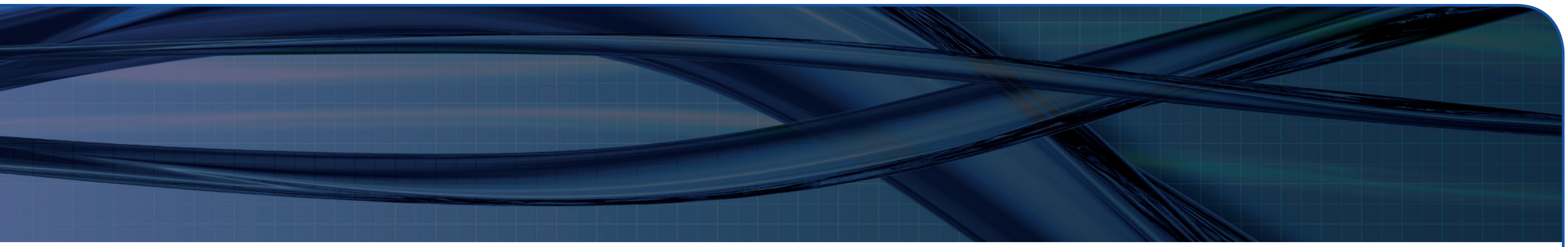
Key Features:

PARAT allows you to:

- Optimally de-identify cross-sectional, longitudinal and geospatial data;
- Assess risk and analyze data handling capabilities;
- Effectively de-identify small local data sets or massive databases on multi-core servers;
- Generate certificates documenting that a data set has a very small risk of re-identification;
- Simulate re-identification attacks in order to test alternative assumptions and do sensitivity analysis;
- Evaluate data quality after de-identification;
- Create custom groupings when standard hierarchies do not exist or are not satisfactory;
- Run many different manipulation\extraction operations on date fields;
- Save and run de-identification specifications to be used on other databases in batch mode or at regular intervals on new data;
- Conduct risk assessments of internal data users or external data recipients on the cloud with the online Risk Assessment Tool;
- Create random sub-samples of data set;
- Use scripting interface to allow external programs and scripts to call PARAT re-identification functions; and
- Discover fields that need to be included in risk measurement and re-identification.

Key Benefits

- Accelerate the process of de-identifying data sets and releasing data;
- Ensure high data utility and data that is acceptable by analysts and increase the number of data releases/year;
- Methods, metrics and algorithms are transparent – peer reviewed;
- Defensible approach and audit trail help you meet regulatory obligations under HIPAA;
- Risk Mitigation – objectively manage your disclosure risks;
- Save days of work in the Privacy Office by automatically generating Data Sharing Agreements; and
- Improved cost effectiveness, compared to doing analysis manually - positive cost of ownership.



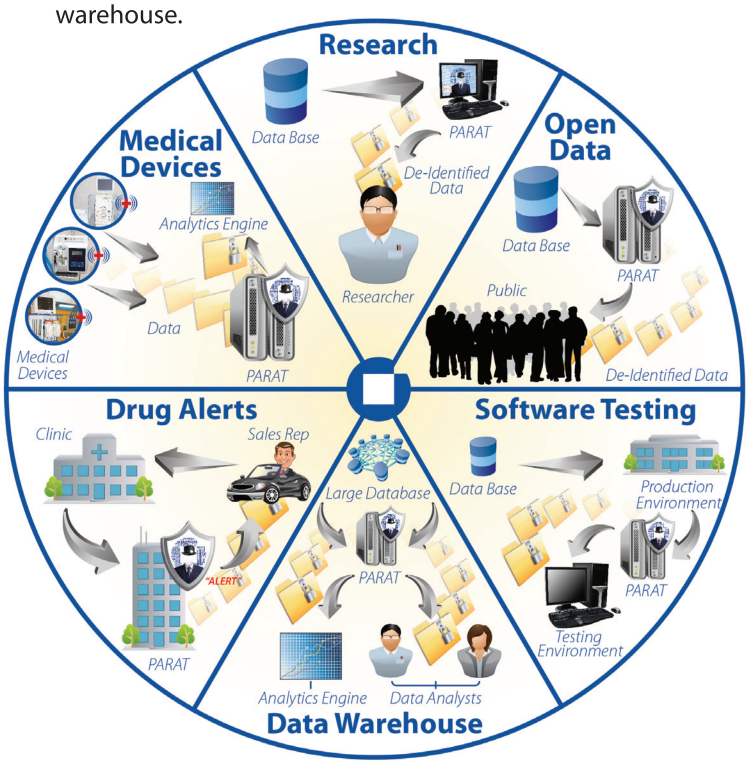
Intelligent Masking

In addition to the de-identification capabilities within PARAT, there also exists intelligent masking functionality which is built specifically for clinical and health claims databases.

Key Features

- Produce realistic test data (i.e. retains the characteristics of the original data) ensuring unusual patterns in the data will also appear during testing;
- Will work on massive databases in a continuous mode for rapid refresh cycles of test data;
- Saves masking function specifications and allows them to be executed again on other databases and at scheduled intervals;
- Includes a library of templates and reference databases for the most common direct identifiers seen in clinical and claims data sets;
- Maintains referential integrity across multiple tables to ensure patient information is masked consistently (i.e. retains the same field type and size);
- Methods ensure that an adversary is unable to reverse engineer masks
- Rapidly processes 100's of GB of data spread across multiple tables

PARAT allows for different deployment scenarios depending on the end use of the de-identified data including research, open data, testing, data warehouses, drug distribution and medical devices. The example below shows how PARAT is deployed and de-identified data is shared in a data warehouse.



Awards

2012 GLOBAL HOT 100
World Summit on INNOVATION & ENTREPRENEURSHIP
THE NEW, SMARTER INNOVATION ECONOMY

Global Hot 100

Gartner 2012 CoolVendor

Gartner Cool Vendor 2012

Gartner Big Data "Cool Vendor in Risk Management, Privacy & Compliance"

O'REILLY® Strata CONFERENCE + HADOOP WORLD
Tools and Techniques That Make Data Work

Strata Conference + Hadoop World Start Up Showcase Winner

PRIVACY ANALYTICS
NOTHING PERSONAL

800 King Edward Drive, Suite 3042
Ottawa, Ontario, Canada K1N 6N5

CONTACT US

www.privacyanalytics.ca | 613.369.4313
info@privacyanalytics.ca