



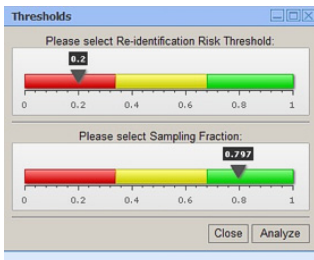
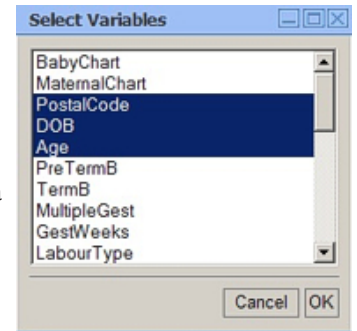
## PRIVACY ANALYTICS RISK ASSESSMENT TOOL (PARAT)

PARAT takes the guesswork out of de-identifying information. Using peer-reviewed metrics and algorithms, PARAT measures and manages re-identification risk. Only PARAT can protect against all known types of re-identification attacks. It optimally de-identifies information to protect individual privacy while retaining the data's value. PARAT is a Windows based application and is compatible with a number of databases (Microsoft Access, Microsoft SQL Server). Using a simple four-step process, PARAT allows you to easily and safely use and disclose your valuable data.

### STEP 1

#### Select the indirect identifiers to be released from the data set

Select the variables that can be used for re-identification. You can rank them in order of importance (the variables' utility to the person using the de-identified data set). This ranking will be used during the de-identification process to determine the optimal anonymization that balances re-identification risk and data utility.



### STEP 2

#### Set your re-identification risk threshold

To balance the need for privacy with the need for data resolution, PARAT allows you to set the acceptable re-identification risk threshold. Re-identification risk can be adjusted based on the profile of the person/organization requesting the information. Risk based de-identification ensures that individual privacy is protected while maintaining the released data's utility.

### STEP 3

#### Perform the Risk Analysis

PARAT calculates the data set's risk for three types of re-identification attacks: prosecutor, journalist and marketer. In this example, PARAT shows the risk is high (above 0.2) for all three types of re-identification attacks (prosecutor, journalist, marketer).

Sample Registry	
Risk results for table	
Prosecutor Risk	High
Journalist Risk	High
Marketer Risk	High
Risk Threshold	0.2
Sampling Fraction	0.8
Dataset Size	
Equivalence Classes	826
Selected Variables	
Postal Code	695
Date of Birth	90
Age	28

Sample Registry	
Risk results for table	
Prosecutor Risk	Low
Journalist Risk	Low
Marketer Risk	Low
Risk Threshold	0.2
Sampling Fraction	0.8
Dataset Size	
Equivalence Classes	39
Selected Variables	
Postal Code	2
Date of Birth	3
Age	11

### STEP 4

#### De-identify to protect data

PARAT uses several de-identification techniques including suppression (removing high risk records) and generalization (reducing the resolution of a given field). PARAT will automatically de-identify the data to reduce the re-identification risk to acceptable levels.

## PARAT: MANAGE RISKS WHILE OPTIMIZING DATA UTILITY

**Custodians:** Health information custodians disclose patient data to registries, researchers, government agencies, and commercial entities without patient consent. By using PARAT custodians ensure that the disclosed data is properly de-identified, complying with privacy laws.

**Data Brokers:** Customer information is valuable market intelligence that is sold to data brokers in the pharmaceutical, financial and insurance industries. In some jurisdictions, data brokers must de-identify the collected data to adhere to privacy legislation. PARAT lowers the risk of exposure and symbolizes a real commitment to privacy.

**Governments:** With precise risk assessments, it's possible for governments to objectively justify information handling decisions, improving risk management and maximizing transparency.

## CONTACT US

[www.privacyanalytics.ca](http://www.privacyanalytics.ca) | 613.369.4313

[info@privacyanalytics.ca](mailto:info@privacyanalytics.ca)

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