Project Closure and Confirmation of Data Destruction Form

Data Analytics Reporting and Evaluation (DARE)

The purpose of this document is to confirm the destruction or return of the extracted data from Data Analytics Reporting and Evaluation (DARE) as per the terms and conditions of the Data Access Agreement with the DARE. A signed Declaration of Destruction Section and confirmation of receipt by DARE on this form constitutes formal closure of the project. Submit the completed form and supporting documents directly to PMR@phsa.ca.

Project Number:

Project Title:

Applicant:

A. Original Media

The original media (e.g. CD, DVD, floppy disk, server access) on which the Data Extract was provided to you by DARE MUST be destroyed using the methods as described in Schedule A. Please complete the following section as applicable.

☐ If the media have been returned to DARE, please provide date:

☐ If the media was destroyed by the Applicant using methods described in Schedule A, please provide the date:

Summary of Original Media Data Destruction:

Please provide details of destruction in the table below.

Data Delivery Date	Data Delivery Contents Title	Data Delivery Type	Destruction Method	Destruction / Return Date
E.g., January 28, 2015	Inpatient shunt operations	CD	Mechanical Shredder	January 28, 2016

Comments:

Project Closure and Confirmation of Data Destruction Form

Data Analytics Reporting and Evaluation (DARE)

Copies of Data and Derived Information

All electronic copies of Data in ALL devices (e.g., desktops, laptops, hard drives) throughout the entire duration of the project, including devices used by all team members with access to the data MUST be destroyed using the methods described in Schedule A. Please complete the following section as applicable.

i. Electronic Copies of the Data and Derived information

☐ Electronic Copies of Data Destroyed.

Important: Data should not be stored on any portable or removable devices (e.g. laptop, memory stick, PDA, etc), regardless of encryption. If you have stored Data on a laptop or an electronic storage device, please follow the Data erasure procedure using the recommended wiping software and continue with Option-1 below.

Option-1 If you have followed the erasure procedure, as recommended by DARE in Schedule A, fill out the following:

Data Storage Location (i.e. Personal Computer & Physical Location/Address):	
Wiping software used:	

☐ Provide data storage path(s) on device noted.

☐ Provide log output from wiping software/erasure program.

Option-2 If you did not use the above noted procedure using the recommended wiping software, please explain in detail your data destruction methods:

"I attest that the methods described above for Data destruction are for ALL THE DEVICES (including CD-ROMS, floppy discs, flash drives, etc. used for backing up files) of all team members with access to the data for the duration of the whole project. I understand that this document is legally binding, and that falsifying this information would constitute a breach of my Data Access Agreement with the DARE and could render me ineligible to access data held by DARE currently and in the future."

Please initial here: ☐

☐ Electronic Copies of Research Data have NOT been destroyed. Please explain:

ii. Paper Records

All paper records of the research extract MUST be destroyed using the methods described in Schedule A.

☐ Paper records have been destroyed. Method:

☐ Paper records have NOT been destroyed. Please explain:

☐ Paper records were not created.

iii. Data in Other Formats

If Data are retained in other formats, please inform us and we will provide you with information on how to properly destroy the Data.

☐ Describe:

Supporting Documentation

If Option 1 for "Electronic Copies of the Data and Derived information" was selected, please provide the following documentation:

- Data storage path(s) on device
- Log output from wiping software/erasure program

Project Closure and Confirmation of Data Destruction Form

Data Analytics Reporting and Evaluation

B. Declaration of Destruction

This document will become a schedule to the Data Access Agreement between DARE and the undersigned approved on: <Date of initial DARE approval>

I, <name> declare that the information provided in this document is accurate, complete and correct. I declare that I have destroyed all original media, copies of the Data, derived information and paper records for the project <project number> as directed by the destruction guidelines and Data Access Agreement in order to officially close the aforementioned project.

Name:

Title:

Organization:

Signature: **Date:**

Witness Name:

Title:

Organization:

Signature: **Date:**

Project Closure and Confirmation of Data Destruction Form

Data Analytics Reporting and Evaluation (DARE)

Schedule A: Guidelines For Data Destruction

The data and any copies (including data in user-restricted network/server folders, all backup and historical copies of the data) must be destroyed using a method of destruction that will render the data unreadable through the use of an appropriate mechanical, physical or electronic process and converted into such a form that cannot be reconstructed in whole or in part.

A. Electronic Copies of the Data from DARE and Derived Information

Electronic copies of Data include all Data and related materials containing Data from DARE or linked records generated with Data from DARE, may include but not limited to the following:

- Derived data
- Duplicated data
- Analysis tables
- Working files
- Backup files
- Data on server
- Temporary files
- Information generated by linking other information to the data
- Data located in files such as word processing documents, spreadsheet workbooks, presentation slides.

i. Magnetic Media (e.g., Hard Drives, Magnetic Tape)

Magnetic media are storage mediums on which digital or analog information is recorded as magnetic signals, such as computer hard drives, magnetic tapes, and floppy disks. For magnetic media and read-write media, either physical destruction or over-writing may be used.

Over-writing is a method used to clear Data from magnetic media that utilizes a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located. To ensure that the original Data is rendered irrecoverable, the areas of the disk holding the Data must be over-written, several times, with random data. The number of overwrites required depends on a number of factors, including the drive type and file system format, but typically, in order to defeat all but the most sophisticated of forensic recoveries, three passes is usually sufficient.

Physical destruction is the preferred sanitization method because this ensures that Data can never be recovered. Mechanical shredding and incineration are such measures used for disposition of sensitive data.

Please note that "regular" deletion of files is not adequate (including the "Empty Trash" feature) - the data still exists on the disk; it is merely the index pointers to the data which are removed in such an operation. The following is an example of a security tool which is effective and readily available.

- MS Windows, MacOS, Linux – BC Wipe (www.jetico.com)

ii. Optical Media (e.g., CD, DVD)

Optical media are storage mediums that hold content in digital form, written and read by laser technology. If there are copies of Data on optical media such as CDs and DVDs, the best approach to destroy the media is physical destruction such as use of a mechanical shredder. Optical media are not magnetic and the Data cannot be overwritten, thus physical destruction is the only choice.

B. Paper Records

Paper records should be destroyed in a manner that leaves no possibility for reconstruction of information. The appropriate method for destroying paper records is cross-cut shredding.