

Exercise 6: Data safety

At the end of this exercise you should be able to:

- a. Backup and encrypt a data file on an external medium.

Nothing should be more valuable to you than the safety of your data. Unfortunately, people often learn that they should have backed up their data only once they have made the painful experience of having lost them.

EpiData Entry can be very helpful and forcing you to back up your data when you close a file. Whether you back up your data to your hard drive (not a good idea in case of hard drive failure) or an external medium, an additional concern is data security. Let's assume you back up your data to a USB flash memory stick and subsequently you lose it. Anybody who finds your stick can look at your data. Perhaps your data contain confidential information that should not be readable by anybody who is not authorized.

EpiData Entry offers password-only accessible encryption tools using so-called strong encryption that cannot be broken without knowing the password you used for encrypting them. We will make a simple EpiData Entry triplet to show how to back up your data with and without encryption to an external medium.

We will use the following simple dataset of the EpiData promoters:

Name	First Name	Country
Rieder	Hans L	Switzerland
Chiang	Chen-Yuan	Taiwan
Hinderaker	Sven Gudmund	Norway
Katamba	Achilles	Uganda
Tun	Zaw Myo	Myanmar
Nguyen	Binh Hoa	Vietnam
Zwahlen	Marcel	Switzerland

Our A_EX06.QES will look as follows:

Questionnaire for back-up data

```
name          <AAAAAAAAAAAAAAAA>
firstname     <AAAAAAAAAAAAAAAA>
country       <AAAAAAAAAAAAAAAA>
```

Make a REC file and a Check file. In the A_EX06.CHK file make all fields MUSTENTER fields, and then open the Check file which should look as follows:

```
name
  MUSTENTER
END
```

```
firstname
  MUSTENTER
END
```

```
country
  MUSTENTER
END
```

Backing up and encrypting your file

Let us assume that your external back-up device takes drive E and has a folder BACKUP on the drive. The command we add in the check file is then:

```
name
  MUSTENTER
END
```

```
firstname
  MUSTENTER
END
```

```
country
  MUSTENTER
END
```

AFTER FILE

```
  BACKUP e:\foldername ENCRYPT filename mypassword TODAY
END
```

The E:\FOLDERNAME is the folder on the drive of your memory stick which you must have created beforehand. FILENAME is the name of the encrypted file and should best be what it is now, i.e. A_EX06 and “mypassword” is a personally chosen password. *Note: if you forget your password, there will be no way to ever open your backup file.* Of course, you can always see it in your original Check file if you choose to keep that. The TODAY function is optional but a good idea to ensure that the current computer date becomes part of the file name. It must be written after the password.

Note: The command BACKUP will back up all files in that folder. Thus, if you wish to backup up only the files A_EX06.* you must first copy those EpiData files that you wish to back up into another empty folder (such as the c:\temp folder after emptying it).

Re-Opening your back-up file

The back-up file will have the name A_EX06.ZKY and will contain not only the REC file but the entire QES-REC-CHK triplet.

In “Tools” you find “Restore archive” and you are prompted to provide the path and name of your archived and encrypted file, to enter your password, and to provide the path where to restore it, with the option to overwrite any existing files.

Task:

- o Create the QES-REC-CHK triplet, edit the Check file, enter the data above and restore the files.*