**SOP Template – Usage of portable devices (USB key, external hard drive, SD card...)**

Data Protection Quick Wins project

***Date of publication :*** *December 2017*

***Author :*** *Quality and Accountability unit*

The aim of this SOP is to define the procedures for delegations concerning the usage of portable devices. This template needs to be adapted by the delegation based on their contextual needs.

1. ***General principles***

* **No sensitive data that is not clearly identified** (ie for back-uping of data, for a mobile data collection etc) **should be stored on a portable device**.
* Most USB keys and SD cards cannot be adequately protected from viruses etc and therefore **should not be used for sensitive data collection, storage or sharing that cannot be lost**.
* **No personal portable device** (USB key or external hard drive) **should ever be used**.
* If you have no other option but to use a **USB key for transfer of sensitive information**, ensure that you **encrypt** the data that you want to store on the USB key and that you delete the data once it is no longer needed.

1. ***initial set-up of devices***

* **When you make data accessible on a portable device** (for back-up, archiving or transfer), **adequate protection measures need to be set up** (encryption, password protection…) that will depend on the risk that a data loss or theft can represent. Password protection is mandatory in all cases.

*Please refer to the “****2.01.*** ***How to choose, store and organise your passwords****” tutorial (part “2. General procedures on access to devices and applications”)*

1. ***Maintenance of devices***

* Ensure that any **data that is no longer needed** is definitively deleted from the relevant portable devices

*Please refer to the “****2.10. How to permanently delete data from your computer or mobile device****” tutorial to know how more.*

* Ensure that any **portable device is restored** when a staff member leaves Tdh or the associated project