Device Encryption Attestation

All University of Utah (U of U) personnel (which includes all faculty, students, staff and U of U affiliates and business associates with a uNID or login account) are required to encrypt data at rest and data in motion for restricted data as classified and published in the data classification model such as PHI, HIPAA &/or human genome Database of Genotypes and Phenotypes (dbGaP).
The data classification and policy can be found at: http://regulations.utah.edu/it/rules/Rule4-004C.php

When storing restricted data on any IT resource or device (e.g., laptops, tablets, desktops, phones, USBs and any type removable media), both university owned or personal, it is required that all devices be cryptographically encrypted with FIPS 140-2 certified standard. Stiff fines to the University can be imposed for each incident of a lost/stolen device which does not have proof of encryption. To have such proof, each device from which the given University personnel stores and/or transmits data classified as restricted is required to have documentation of having an appropriate encryption method implemented.

All such devices should be listed below, along with the method of encryption, and be verified by your home IT department. If you obtain a new device, you must obtain a new attestation of encryption.

The completed document must be stored in a safe place for reference. It is recommended that a copy be filed with your home department as well as that you keep a copy for your own record. This document will serve as attestation for proof of device encryption in the event that the device is lost or stolen.

As a University of Utah personnel, I certify that the below computers and portable devices have been verified to be encrypted and satisfy Restricted data security requirements as of the given date.

_____ _____ _____
1ST IT resource/device Serial or IMEI # **Device MAC address** **Device type/description**

_____ _____ _____
Department Encryption Method Date

_____ _____ _____
2nd IT resource/device Serial or IMEI # **Device MAC address** **Device type/description**

_____ _____ _____
Department Encryption Method Date

_____ _____ _____
3rd IT resource/device Serial or IMEI# **Device MAC address** **Device type/description**

_____ _____ _____
Department Encryption Method Date

As a University Personnel, I certify that I understand the above and will not access dbGaP or other Restricted/PHI data on UofU CHPC servers remotely or from any computer or portable device not certified above.

_____/_____ _____
IT resource/device user/owner/operator printed name & Signature Date

_____/_____ _____
IT admin or home department witness verification printed name & Signature Date

Document Last edited 10/7/2016