**Data Security Standards for Compliant Data Obtained for Research Purposes**

Per the University of Maine System (UMS) Information Security Standards, compliant data are defined as: ***Information which has specified requirements for the control of confidentiality, availability, or integrity of the data due to statute or contract or other law or agreement. Compliant data is information which requires special protection because the misuse could harm members of the UMS community or compromise the mission of the System and/or any one of the Universities. Compliant data includes, but is not limited to, personally-identifiable information, confidential research information, and information that requires protection under law or agreement such as the Maine Data Act, FERPA (the Family Educational Rights and Privacy Act), GLBA (the Gramm-Leach Bliley Act), HIPAA (the Health Insurance Portability and Accountability Act), FTC "Red Flag Rule", -by the PCI (Payment Card Industry) data security standards, and data placed on legal hold in accordance with e-discovery. Examples of Compliant Data include: financial records, health records, student educational records, and any information which could permit a person to attempt to harm or assume the identity of an individual.***

Data must be labeled and handled as follows:

At the University of Southern Maine electronic compliant data is stored on a dedicated network drive, referred to as the compliant network drive hereafter, separate from the standard departmental and user network drives. The compliant network drive may only be accessed from University owned computers that have USM's Virtual Private Network (VPN) software installed. The compliant network drive and VPN software provide additional technical safeguards that are necessary for the storage of compliant data.

Storage space on the compliant network drive can be requested by contacting the USM HelpDesk. Space will be allocated at a cost of $5 per 5 Gigabyte of disk space per month. Before space can be allocated, an UMS Chartfield Combo to which the monthly charge will be billed must be provided along with a list of the user accounts that will need access to the newly allocate space.

Once space has been allocated, the VPN software can be installed on the University owned computers from which the data will be accessed. Each user must sign USM's VPN agreement before they can use the VPN. The HelpDesk will provide copies of the agreement. Prompt return of the agreement will help avoid delays in the VPN setup process. Additionally, any laptop computer that will be used to access the compliant network drive must have its hard drive encrypted. This will be done by the HelpDesk as well.

Once setup is complete, users can access the compliant network drive by logging in to their computers, opening the VPN software, logging in to the VPN, and then connecting to the compliant network drive. Once connected, the compliant network drive can be used like other network drives.

Access to data is limited to only those persons listed in the Institutional Review Board (IRB) approved protocol. Requests for additional access should be requested via the Protocol Revision and Amendment Form on the IRB website and approved before access is permitted.

When transmitting Compliant Data to a recipient outside the UMS, the sender must be sure that the recipient understands that the data is Complaint Data, and is authorized to receive such data.

The information must be protected according to any additional requirements of the IRB and/or contract or agreement pertaining to the information.

If there is reason to believe that storing and accessing compliant data via the mechanism outlined here is not compatible with the business or research process for which the data is being used, alternative means of storing and accessing the data may be used. However, all methods of storage and access that deviate from those described here must be approved by the IRB, the Chief Information Officer of the University of Southern Maine, and the Chief Information Security Officer of the University of Maine System to insure that they meet all applicable statutes, contracts, other laws, and agreements.

Reference: University of Maine System Information Security Standards accessed November 17, 2011.