Data Security Standards for Business Sensitive Data Obtained for Research Purposes

Per the University of Maine System (UMS) Information Security Standards, business sensitive data are defined as: ***Information that is not the subject of statutory or contractual controls, but where compromise of the confidentiality, integrity, or availability of the information would result in damage or loss to UMS.***

Data must be labeled and handled as follows:

Data must be protected in a system that requires a password to access. Folders on departmental or user network drives that have been limited to approved persons can be used for this type of data.

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 Business Sensitive Data to a recipient outside the UMS, the sender must be sure that the recipient understands that the data is Business Sensitive Data, and is authorized to receive such data. The information must be protected according to any additional requirements of the IRB and/or contract pertaining to the information.

If there is reason to believe that storing and accessing business sensitive 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 Policy and Security Standards accessed November 17, 2011.