

Community Investment Guideline Data Security for COMET

United Way must protect restricted, confidential and sensitive data to retain the public trust, avoid reputation damage and avoid adversely impacting the people that we serve. We expect all Community Fund partner agencies to share this commitment to information protection. This is particularly critical for all agencies participating in United Way strategy evaluation using COMET. COMET is the web-based information system which houses data on individuals served by funded projects. Some of the data included in the system is protected information in that it is subject to Federal, State and local regulations such as HIPPA, FERPA and NYS Breach Notification.

To increase COMET user awareness of the importance of data security and to avoid accidental loss we expect all users in United Way sponsored COMET projects to:

- Create security policy and procedures to govern the access, use and disclosure of all protected information.
- Limit access to protected information to personnel who require access in the performance of their job function.
- Provide security training on the importance of and how-to's of data security.
- Install technical protections for all electronic data. This includes the use of a firewall and Intrusion Detection System to protect external access as well as installation of Anti-Virus/Anti-Spam software on all computers.
- Transfer data using secure transfer mechanisms only (e.g. using encrypted email when identifying data is sent).
- Provide notification to the United Way's COMET Administrator, Elizabeth Ramsay Marchese, if any information has been compromised or there has been unauthorized disclosure of protected information.