Appendix D. REL Midwest CLC Study – MDRC Confidentiality Agreement Template

MDRC's Confidentiality Protocol

MDRC is committed to protecting the security and confidentiality of data. The following policies and procedures must be employed by all MDRC staff handling data.

- **Confidentiality agreements:** All staff must sign an agreement to abide by the corporate policies on data security and confidentiality. This agreement, signed at the start of employment and renewed periodically thereafter, affirms each individual's understanding of the importance of maintaining data security and confidentiality, and abiding by the management and technical procedures that implement these policies. Subcontractors, consultants and other nonpermanent staff must also sign agreements requiring data confidentiality and security.
- **Data security, paper files:** All individually-identifiable data received in paper documents must be logged and stored in locked storage areas with limited access on a need to know basis. Staff must black out identification items when distributing paper documents to broader audiences as samples.
- **Data security, computerized files:** MDRC has developed a robust technical environment, secured by firewalls, that limit access to designated network areas and requires authorized individuals to gain access via password identification systems. In the event that data files containing items identifying individuals must be transmitted between MDRC's own network system and another location (such as government agency or service provider, or subcontractor), encryption with passwords should be used to assure file security and data integrity.
- **Data management:** MDRC's network provides centralized services for data storage and processing, thus avoiding proliferation of file copies to multiple workstations. Source data received on electronic media (tapes, cartridges, diskettes, etc.) should be transferred into the appropriate limited access sections of the network, and the media should be secured in locked storage.
- **Merged data:** MDRC recognizes that merged data sources present additional risks of identification of individuals. It is MDRC policy to strip identification data from files before merging to preclude overt identification of individuals. In addition, data should be cleaned, grouped or aggregated when combinations of items from different sources create a risk of identification of individuals.
- **Data presentation:** All reports, tables and printed materials are limited to presentation of aggregate numbers. Data lists generated to conduct data assessments or data inquires are restricted in distribution on a need-to-know basis and destroyed upon completion of usage.
- **Limitations on data sharing:** Compilations of individualized data may not be provided to participating agencies, unless research subjects specifically grant consent for this disclosure.
- **Data retention:** MDRC retains both electronic and paper archives of project material subsequent to the completion of a project. The time of archiving depends on contractual requirements. Access to archive areas, paper or electronic, is restricted to authorized individuals only.
- **Data destruction:** After the completion of a project, media containing individually-identifiable records must be destroyed by an appropriate fail-safe method, including physical destruction of the media itself or destruction of the contents of electronic media.