202. Security and Protection of Not-Public Data on Individuals

Clearwater River Watershed District establishes the following protocols pursuant to and in satisfaction of the requirement in Minnesota Statutes section 13.05, subdivision 5, that CRWD establish procedures ensuring appropriate access to not-public data on individuals. CRWD has no employees; the CRWD administrator is a contractor. The administrator has access to and manages access by others to all not-public CRWD data in accordance with the following protocols.

Implementing Procedures

Since it has no employees, CRWD regularly creates, receives and maintains very little not-public data on individuals. CRWD managers, the administrator (as Responsible Authority/Data Practices Compliance Official) and counsel may have access to any not-public data created, received or maintained by CRWD as necessary for specified duties. Any access to not-public data will be strictly limited to the data necessary to complete the work assignment.

Data sharing with authorized entities or individuals

State or federal law may authorize the sharing of not-public data in specific circumstances. Not-public data may be shared with another entity if federal or state law allows or mandates it. Individuals will be provided with notice of any sharing in an applicable Tennessen warning or CRWD will obtain the individual's informed consent. Any sharing of not-public data will be strictly limited to the data necessary or required to comply with the applicable law.

To ensure appropriate access, CRWD will:

- Assign appropriate security roles, limit access to appropriate shared network drives and implement password protections for not-public electronic data
- Password protect the administrator's computer and lock the computer before leaving the workstation
- Secure not-public data within locked work spaces and in locked file cabinets
- Shred not-public documents before disposing of them

Penalties for unlawfully accessing not-public data

CRWD will impose, as necessary, penalties for unlawful access to not-public data as provided for in Minnesota Statutes section 13.09. Possible penalties include suspension, dismissal or referring the matter to the appropriate prosecutorial authority who may pursue a criminal misdemeanor charge.

Protection of Private and Confidential Data on Individuals

Data Safeguards

Private and confidential information is stored in secure files and databases that are not accessible to individuals who do not have authorized access. Private and confidential data on individuals is accessed only by individuals who are both authorized and have a need to access such information for CRWD purposes. (An individual who is the subject of data classified as private may access such data for any reason.)

The CRWD administrator, as Responsible Authority, reviews forms used by CRWD to collect data on individuals and ensures that CRWD collects private or confidential data only as necessary for authorized CRWD purposes.

Only managers and the administrator may access files and records containing such information. The administrator's and managers' access is further governed by the following requirements:

- Private or confidential data may be released only to persons authorized by law to access such data
- Private or confidential data must be secured at all times and not left in a location where they may be accessed by unauthorized persons
- Private or confidential data must be shredded before it is disposed of

When a contract with an outside entity requires access to private or confidential information retained by CRWD, the contracting entity is required by the terms of its agreement with CRWD to use and disseminate such information in a manner consistent with the DPA and CRWD's Policies and Procedures for Public Access to Documents.