Privacy and Security Policy

Each sub-recipient must designate a Chief Policy Officer, which shall be an administrator who will conduct the training in the contents of the Privacy and Security Notice Manual and who will handle questions and complaints about the Privacy Notice.

The Personnel Manual must state that all employees, volunteers, and Board members who collect, read, or are otherwise exposed to client information will be trained in the contents of the Privacy and Security Notice Manual. Each person and the Chief Policy Officer will sign the Employee/Volunteer/Board Member Acknowledgement of Privacy Notice and Certification of Training contained in the Privacy and Security Notice Manual. These will be kept either in the employee's personnel file, or in the case of volunteers and Board members, on file in the Director's office.

The Privacy and Security Notice to the Public must be posted next to each intake desk and in all common client areas. All computer monitors visible from a common area must face away from the common area to preserve client privacy.

All computers must have virus protection with automatic updates. All sub-recipients must have a firewall on the network and/or workstation(s) to protect the HMIS system from outside intrusion. If the Sub-recipient maintains a web site, the Privacy and Security Notice must be posted on the home page.

The HMIS Database Administrator (MISI, Inc.) must have unrestricted administrative access to all of the sub-recipient's computers that are connected to the HMIS database, to check for safety and security features such as virus protection and firewalls.

_____

Staff Signature and Date