F. Work Conditions and Hours

1. Safety

To assist in providing a safe and healthful work environment for employees, clients, and visitors, the Clinic has established a workplace safety program. Management has responsibility for implementing, administering, monitoring, and evaluating the safety program. Its success depends on the alertness and personal commitment of all.

The Clinic provides information to employees about workplace safety and health issues through regular internal communication channels such as management-employee meetings, bulletin board postings, memos, or other written and/or verbal communications.

Employees receive periodic workplace safety training. The training covers potential safety and health hazards and safe work practices and procedures to eliminate hazards.

Some of the best safety improvement ideas come from employees. Those with ideas, concerns, or suggestions for improved safety in the workplace are encouraged to raise them with someone in management who will direct them to the proper person or take action to correct the situation themselves. Reports and concerns about workplace safety issues may be made without fear of reprisal.

Each employee is expected to obey safety rules and to exercise caution in all work activities. Employees must immediately report any unsafe condition to a member of management. Employees who violate safety standards, who cause hazardous or dangerous situations, or who fail to report or where appropriate, remedy such situations, may be subject to disciplinary action, up to and including discharge from employment.

In the case of accidents that result in injury, regardless of how insignificant the injury may appear, employees should immediately notify a member of management. Such reports are necessary to comply with laws and initiate insurance and Workers' Compensation benefits procedures.

2. Smoking

In keeping with the Clinic's intent to provide a safe and healthy environment for patients, clients, visitors, and employees at the Clinic, smoking in the workplace is prohibited. In situations, whether at work or at a Clinic function, where the preferences of smokers and nonsmokers are in direct conflict, the preferences of nonsmokers will prevail.

This policy applies equally to all employees, clients, and visitors.

3. Use of Equipment

Equipment essential in accomplishing job duties is often expensive and may be difficult to replace. When using properly, employees are expected to exercise care, perform required maintenance, and follow all operating instructions, safety standards, and guidelines.

Please notify a member of management if any equipment, machines, or tools appear to be damaged, defective, or in need of repair. Prompt reporting of damages, defects, and the need for repairs could prevent deterioration of equipment and possible injury to employees or others. A member of management can answer any questions about an employee's responsibility for maintenance and care of equipment used on the job.

The improper, careless, negligent, destructive, or unsafe use or operation of equipment can result in disciplinary action, up to and including discharge from employment as well as possible reimbursement payable to the Clinic for repair or replacement of the damaged piece(s).

4. Visitors in the Clinic

To provide for the safety and security of employees and the facilities at the Clinic, only authorized visitors are allowed in the workplace. Restricting unauthorized visitors helps maintain safety standards, protects against theft, ensures security of equipment, protects confidential information, safeguards employee welfare, and avoids potential distractions and disturbances.

All visitors should enter the Clinic at the main entrance. Authorized visitors will receive directions or be escorted to their destination. Employees are responsible for the conduct and safety of their visitors.

If an unauthorized individual is observed on the Clinic's premises, employees should immediately notify a member of management or, if necessary, direct the individual to the main entrance.

5. The "Technology Policies"

Use of Telephones

Personal use of the telephones for long-distance and toll calls is not permitted. Employees should practice discretion in using Clinic telephones when making or receiving local personal calls and may be required to reimburse the Clinic for any charges resulting from their personal use of the telephone.

To ensure effective telephone communications, employees should always use the approved greeting and speak in a courteous and professional manner. Please confirm information received from the caller, and hang up only after the caller has done so.

Use of Postal Machine, Fax Machine, E-Mail, the Internet, Voice Mail, and Computer Network

The use of the Clinic's automation systems, including computers, postal machine, fax machine, and all forms of Internet/Intranet access, is for Clinic business and is to be used for authorized purposes only. Personal use of the postage machine (including postage stamps) is prohibited. Brief and occasional personal use of the fax machine, electronic mail system or the

Internet is acceptable as long as it is not excessive or inappropriate, occurs during personal time (lunch or other breaks, or before or after regular work hours), and does not result in expense to the Clinic.

Use is defined as "excessive' if it interferes with normal job duties, responsiveness, or the ability to perform daily job activities. The Clinic automation systems are Clinic resources and are provided as business communications tools. Electronic communication should not be used to solicit or sell products, distract co-workers, or disrupt the workplace.

Use of the Clinic computers, network, and Internet access is a privilege granted by management and may be revoked at any time for inappropriate conduct including, but not limited to:

- Sending chain letters;
- Engaging in private or personal business activities;
- Misrepresenting oneself or the Clinic;
- Engaging in unlawful or malicious activities;
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;
- Sending, receiving, or accessing pornographic materials;
- Becoming involved in partisan politics;
- Causing congestion, disruption, disablement, alteration, or impairment of the Clinic network or systems;
- Using recreational games;
- Defeating or attempting to defeat security restrictions on Clinic systems and applications;
- Downloading/installing programs (including email attachments) to any Clinic system without the consent of management; and/or
- Accessing unsafe or unreliable Internet sites.

Using Clinic automation systems to create, view, transmit, or receive racist, sexist, threatening, or otherwise objectionable or illegal material is strictly prohibited. "Material" is defined as any visual, textual, or auditory entry. Such material violates the Clinic's anti-harassment policies and is subject to disciplinary action. The Clinic's electronic mail system must not be used to violate the laws and regulations of the United States or any other nation or state, city, province, or other local jurisdiction in any way. Use of Clinic resources for illegal activity can lead to disciplinary action, up to and including discharge from employment and criminal prosecution. Unless specifically granted in this policy, any nonbusiness use of the Clinic's automation systems is expressly forbidden. Violations of these policies could subject an employee to disciplinary action, up to and including discharge from employment.

Ownership and Access of Electronic Mail and Computer Files

The Clinic owns the rights to all data and files in any computer, network, or other information system used in the Clinic. The Clinic also reserves the right to monitor electronic mail messages and their content. Employees must be aware that the electronic mail messages that they send and receive using the Clinic equipment are not private and are subject to viewing,

downloading, inspection, release, and archiving by the Clinic officials at all times. No employee may access another employee's computer, computer files, or electronic mail messages without prior authorization from either the employee or someone in management.

The Clinic has licensed the use of certain commercial software application programs for business purposes. Third parties retain the ownership and distribution rights to such software. No employee may create, use or distribute copies of such software that are not in compliance with the license agreements for the software. Violations of this policy can lead to disciplinary action, up to and including discharge from employment.

Confidentiality of Electronic Mail

As noted above, electronic mail is subject at all times to monitoring and the release of specific information is subject to applicable state and federal laws and Clinic rules, policies, and procedures on confidentiality. Existing rules, policies, and procedures governing the sharing of confidential information also apply to the sharing of information via commercial software. Since there is the possibility that any message could be shared with or without your permission or knowledge, the best rule to follow in the use of electronic mail for nonworker related information is to decide if you would post the information on the office bulletin board with your signature.

It is a violation of the Clinic policy for any employee to access electronic mail and computer systems files to satisfy curiosity about the affairs of others. Employees found to have engaged in such activities may be subject to disciplinary action, up to and including discharge from employment.

Electronic Mail Tampering

Electronic mail messages received should not be altered without the sender's permission nor should electronic mail be altered and forwarded to another user and/or unauthorized attachments be placed on another's electronic mail message.

Policy Statement for Internet/Intranet Browser(s)

This policy applies to all uses of the Internet, but does not supercede any state or federal laws or Clinic policies regarding confidentiality, information dissemination, or standards of conduct. The use of the Clinic automation systems is for business purposes only. Brief and occasional personal use is acceptable as long as it is not excessive or inappropriate, occurs during personal time (lunch or other breaks), and does not result in expense to the Clinic. Use is defined as "excessive' if it interferes with normal job functions, responsiveness, or the ability to perform daily job activities. Examples of inappropriate use are defined above. The Clinic's management will determine the appropriateness of the use and whether such use is excessive.

The Internet is to be used to further the Clinic's mission, to provide effective service of the highest quality to the Clinic's clients and staff and to support other direct job-related purposes. Management should work with employees to determine the appropriateness of using the

Internet for professional activities and career development. The various modes of Internet/Intranet access are the Clinic's resources and are provided as business tools to employees who may use them for research, professional development and work-related communications. Limited personal use of Internet resources is a special exception to the general prohibition against the personal use of the Clinic computer equipment and software.

Employees are individually liable for any and all damages incurred as a result of violating Clinic security policy, copyright, and licensing agreements. All the Clinic policies and procedures apply to employees' conduct on the Internet, especially but not exclusively, relating to: intellectual property, confidentiality, Clinic information dissemination, standards of conduct, misuse of Clinic resources, anti-harassment and information, and data security. Violation of these policies and/or state and federal laws can lead to disciplinary action, up to and including discharge from employment and possible criminal prosecution.

Internet/Intranet Security

The Clinic owns the rights to all data and files in any information system used in the Clinic. Internet use is not confidential and no rights to privacy exist. The Clinic reserves the right to monitor Internet/Intranet usage, both as it occurs and in the form of account histories and their content. The Clinic has the right to inspect any and all files stored in private areas of the network in order to assure compliance with policy and state and federal laws. The Clinic will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual Internet activities. Existing rules, policies, and procedures governing the sharing of work-related or other confidential information also apply to the sharing of information via the Internet/Intranet. Any employee who attempts to disable, defeat, or circumvent the Clinic security measures may be subject to disciplinary action, up to and including discharge from employment.

Employees are also expected to exercise discretion when accessing Internet sites. Only Internet sites that are reasonably believed to be safe, reliable and pose no risk to any of the Clinic's systems may be accessed.

Downloading/Installing Programs

Due to the increased security risk of computer viruses, spy ware and incompatibility issues, employees are not to download any program (including email attachments) from the Internet nor install any software application without the consent of management. Failure to comply with this policy may subject an employee to disciplinary action, up to and including discharge from employment.

Use of Social Networking Sites

With social networking on sites such as Facebook.com, Twitter.com, MySpace.com, etc. being commonly used in today's culture, it is expected for employees to use discretion in what they post on their personal social network site as well as the social network site of others to avoid damaging the reputation of the Clinic, clients, employees, vendors and competitors. Like all internet usage, accessing social networking sites is to be of limited use during work hours as

described above. Violations of this policy can lead to disciplinary action, up to and including discharge from employment as well as subject the employee to possible criminal prosecution for defamation of character or other harm.

User Accounts and Passwords

User accounts and passwords are individually assigned to protect the integrity of information and to identify the person performing a specific function. Therefore, user accounts and passwords are private and are not to be copied, stored or shared with anyone. If, though, at any time you believe your user account or password has been compromised, notify management immediately. Violations of this policy can lead to disciplinary action, up to and including discharge from employment as well as subject the employee to possible criminal prosecution in the event the misuse of a user account/password causes harm to another person.

6. Confidentiality

Clinic employees may know important personal and financial information about clients, management, and fellow employees. It is absolutely essential that we guard the confidentiality of any such information in our possession. This means that you should not disclose confidential information unless you are authorized to do so by the person(s) involved or management. Any violation of confidentiality may result in disciplinary action, up to and including discharge from employment.

7. Work Schedules

Work schedules for employees vary throughout the Clinic. Management will advise employees of their individual work schedules. Staffing needs and operational demands may necessitate variations in starting and ending times, as well as variations in the total hours that may be scheduled each day and week. This may include a person in management sending employee(s) home early on days in which there is little or no workload. No compensation will be paid to nonexempt employees sent home early.

An employee must receive approval from management before making up any missed time or before switching work schedules with a co-worker. In addition, any approved make-up time must be completed in the same week as time was missed. This helps ensure that the staffing and workload needs of the clinic are properly met.

8. Rest and Meal Periods

Each workday, nonexempt employees are provided with a 15-minute rest period for every 4 hours worked in a day. To the extent possible, rest periods will be provided in the middle of work periods. Since this time is counted and paid as time worked, employees must not be absent from their workstations beyond the allotted rest period time.

All full-time, nonexempt employees are provided with one 30-minute meal period each workday. If the employee remains available to work during the meal period, the employee does not have to clock out and back in for the meal period. If the employee will not be

available for their work responsibilities during the meal period, they will not be compensated for that meal period and will need to clock out at the start of the meal period and in again at the return from the meal period.

9. Overtime

When operating requirements or other needs cannot be met during regular working hours, employees will be given the opportunity to volunteer for overtime work assignments. All overtime work must receive the prior approval from management. Overtime assignments will be distributed as equitably as practical to all employees qualified to perform the required work. Overtime compensation is paid to all nonexempt employees, in accordance with federal and state wage and hour restrictions. Overtime pay is based on actual hours worked. Time off on sick leave, vacation leave, holiday, bereavement leave, or any leave of absence will not be considered hours worked for purposes of performing overtime calculations.

Failure to work scheduled overtime or overtime worked without prior authorization from management may result in disciplinary action, up to and including discharge from employment.