HEP-C ALERT, INC.
GENERAL INFORMATION SECURITY POLICY

A. SECURITY OVERVIEW

1. General Quality Assurance.

1.1. Information security activities are monitored periodically by the Security Coordinator to ensure compliance with policy, protocol and procedures.

2. Description of "Confidential Information."

2.1. Confidential Information is any material or information which contains a client name.

2.2. Confidential information includes but is not limited to: client call-back reports; contact sheets; support group attendance forms; counseling and testing intake and risk assessment forms; test results; referral forms; counseling notes and any client information appearing on computer screens.

3. Description of "Information Security."

3.1. Information Security means that all client information is maintained in a secured manner and safeguarded at all times from unauthorized access.

3.1.1. Confidential information is never left unattended, including unattended computer monitors open to a client account.

3.1.2. Both paper and electronic information is maintained and stored in secured areas and in a manner that limits access.

3.1.3. Unauthorized persons are always escorted and not left unattended in areas where confidential information is maintained.

4. Physical Security.

4.1. The office is protected by a security alarm. Motion detectors are located in the front counseling office, reception area and rear hallway. The front and back door of the office remain locked at all times.

4.2. Clients ring the doorbell and are either accompanied by a staff member at all times or remain in a counseling room with the door closed until a counselor becomes available.

4.3. Office doors have pneumatic door closures, locking handles, and at least one locking file cabinet or drawer for temporary secure storage.

4.4. A Secure Records Room is designated with a locking handle, a deadbolt combination lock and a locking file cabinet with a padlocked security bar.

4.5. A Secure Computer Room is designated with a locking handle, a deadbolt lock.

5. Contingency Planning

5.1. Refer to Hep-C ALERT's Hurricane Preparedness Plan.

6. Employee Roles and Responsibilities.

6.1. Security Coordinator: The Office Manager is the Security Coordinator. He/She has the specific responsibility to coordinate the security of information for the purposes of protecting confidentiality, data integrity and appropriate access to information. These responsibilities are documented in his/her personnel folder.

6.2. Information Custodian: The Project Assistant is the Information Custodian for hard-copy information. The Office Manager is the Information Custodian for electronic information. They have the responsibility for securing their designated information set for the purposes of protecting confidentiality, data integrity and appropriate access. These responsibilities are documented in their personnel folder.

6.3. Employees with "Need To Know": The need to know is limited to those persons whose jobs could not be performed without access to the confidential information. “Need to know” for an individual employee or volunteer is established by the Director and documented. The identity of employees with Need To Know are attached in Addendum 1. These responsibilities are documented in their personnel folder.

6.4. Key Custodian: A Key Custodian is designated for each secure area. Secure Records Room Key Custodians are the Project Assistant and the Office Manager. Secure Computer Room Key Custodian is the Office Manager. Custodians are responsible for maintaining control of the keys, providing keys to authorized persons and otherwise allowing access to the area. Documentation is for the number of keys distributed. No key is provided for persons not on the list of personnel with authorized access. Documentation includes the signature of the person receiving the key. These responsibilities are documented in their personnel folder.

6.5. Disclosure of Test Results: Test result notification for HIV is restricted to staff with current HIV 501 Certification through the Florida Department of Health, Bureau of HIV/AIDS. Test result notification for HCV is limited to staff with HIV 104 or greater training, and certificate of successful completion of the CDC Hepatitis C CD-rom training course OR Hep-C ALERT's 8-hour Peer Counselor Certification Training. Documentation of training is documented in the personnel folder.

7. Confidentiality and Security Statement of Understanding.

7.1. Every staff member signs a Confidentiality and Security Statement of Understanding.

8. Security Awareness Training and Frequency.

8.1. Every staff member attends the Security Awareness Training and Training Updates.

B. COMMUNICATIONS SECURITY

1. Communication Quality Assurance.

1.1. Internal and external communications are monitored periodically by the Security Coordinator to ensure compliance with policy, protocol and procedures.

2. Answering Phones.

2.1. The switchboard is answered using "ALERT [staffmember] speaking, are you calling to speak with a counselor OR how may I direct your call?

2.2. Staff answers their extension using "This is [staffmember]. How may I help you?".

3. Verbal Communications.

3.1. Phone calls to clients or conversations between staff members concerning confidential client information are conducted private offices to ensure confidentiality.

3.2. Staff may contact clients by phone using "This is [staffmember] from ALERT calling…".

3.3. Staff may not call a client regarding an HIV appointment or test result under any circumstances unless the client consented for this in writing.

3.4. These procedures and documentation shall not designate specific services which would compromise the client’s confidentiality.

4. Counseling/Testing Appointment Sign-in Sheets.

4.1. Sign-in sheets contain only the time the client arrived and their name.

4.2. To protect the client’s confidentiality, client names are not used when calling the client to a room for counseling.

4.3. If more than one client is waiting for counseling, a number is assigned and the client called for their appointment by that number.

5. Faxing.

5.1. HIV client information is never received or sent by fax. HCV client information may be sent and/or received with appropriate Records Release (see Section E-2).

5.2. A fax coversheet containing the warning found in DOH Security Policy 7.1.V(F) is used for all faxes (whether confidential or not).

6. **Mailing.**

6.1. Any and all HIV confidential information is double enveloped for mailing.

6.2. Only HCV confidential information mailed for monthly reporting to the Department of Health is double enveloped.

6.2.1. The interior envelope includes the word "Confidential" and the intended recipient's name (and department if applicable).

6.2.2. The exterior envelope is addressed according to USPS addressing standards and includes the word "Confidential" on the lower left corner of the envelope.

6.3. HCV confidential information mailed to clients (if requested) is single enveloped, sealed and taped shut at the seam.

C. PAPERWORK SECURITY

1. Printing and Tracking Quality Assurance.

1.1. Logging and tracking of reports and files from confidential databases is implemented and reviewed periodically by the Security Coordinator to ensure compliance with policy, protocol and procedures.

2. Document Storage.

2.1. All hard copy confidential client information is maintained in a file cabinet or file drawer that is locked at all times when not in use.

2.2. The custodian of the key-code for the Secure Records Room is also the custodian of the key for the locking file system. Those with key access to the files are designated in the security procedures.

3. Printer Security.

3.1. The network printer is not in a secure area.

3.2. Confidential information is printed only when the printer is directly monitored by an authorized staff member.

4. Printing Reports Containing Confidential Information.

4.1. For the purpose of this policy, the term "Report" refers to any document containing more than one client record.

4.2. Only authorized staff may print reports from the HIMS™ Reports Menu.

4.3. Querying and/or printing anything containing client information through any other means is strictly prohibited and may be cause for disciplinary action.

4.4. Reports contain only the minimum information needed to effectively perform work assignments and use an ambiguous header/title to avoid identifying the status of the clients listed.

5. Report Security Log.

5.1. A Report Security Log is maintained next to the network printer.

5.2. The staff member printing the report writes their name; date printed; report title; and the name of the staff member responsible for the report (if different).

5.3. The staff member responsible maintains the report in accordance with all security and confidentiality policies, protocols and procedures.

6. Documenting Report Disposal.

6.1. When finished with the report, the staff member responsible for the report writes the date the report was properly disposed on the Report Security Log, then places the report into the secure document destruction bin.

7. Scheduling Document Disposal Services.

7.1. The Security Coordinator checks the document destruction bin monthly.

7.2. When the bin is 3/4 full, he/she contacts American Document Destruction Corporation at 800-745-2332 for removal and a new locking container.

7.3. Prior to annual archival activities, the Security Coordinator contacts American Document Destruction Corporation to increase secured document disposal capacity.

8. Requesting Client Charts/Records For Counseling and Testing.

8.1. Only one client chart per staff member may be checked out from the Secure Records Room at a time for the purpose of for counseling and testing. Exceptions require the authorization of the Security Coordinator, HIV Testing Director or the Executive Director.

8.2. A Record Transaction Log is maintained in the Secure Records Room. The staff member requesting the file writes their name, the client name, date and reason for request. The Record Custodian checks the file out to the staff member.

8.3. The staff member responsible maintains the chart in accordance with all security and confidentiality policies, protocols and procedures.

8.4. Confidential information is always carried by hand in an opaque file folder that does not identify the contents as containing HIV and/or HCV positive results.

9. Security During Operating Hours.

9.1. Confidential paperwork used for client services is safeguarded at all times.

9.2. When staff leave their workstation (even for a moment), they place confidential information in a closed drawer or closed overhead bin.

9.3. Staff leaving a work area which is unattended altogether, locks their office door on exit.

10. Security After Operating Hours.

10.1. All confidential client information as well as the document destruction bin, is stored in the Secure Records Room at 5:00pm every business day.

10.2. If some confidential records are required for client services after 5:00pm, they are secured at the close of business by placing in a clasp envelope and sliding under the door of the Secure Records Room before exiting the office.

10.3. The last staff member to leave the office ensures file drawers and doors are locked, then sets the security alarm before leaving.

11. Security Before/During/After Field Services

11.1. Only authorized staff conducts field counseling/testing/referral services. Confidential information is maintained in a locked briefcase at all times.

11.2. Authorized staff uses the minimum of information needed to complete services, then returns the information to the Secure Records Room after the specified period of time. In the event of unforeseen circumstances that prohibit the return of confidential information from the field to the office by the end of the business day or authorized field services period, staff telephones the HIV Program Director or Executive Director to advise.

11.3. Authorized staff takes reasonable and prudent care to safeguard the information, including removing it from their vehicles and maintaining it in their home.

D. RELEASE OF INFORMATION AND RECORDS RETENTION SECURITY

1. Release of Information Quality Assurance.

1.1. Release of confidential information activity is monitored periodically by the Security Coordinator to ensure compliance with policy, protocol and procedures.

2. General Policy For Release of Confidential Information.

2.1. Confidential information is never released to any party other than the client him/herself. This includes HIV and/or HCV test result information.

2.2. A client requests their information in person, and presents a valid photo ID that includes a visible signature. Staff checks the photo ID to verify identity before releasing information, including prior to providing test results during post-test counseling.

3. Release of HCV Confidential Information.

3.1. A HCV test result may be released by mail or fax (to either a client or provider) providing these stipulations are met:

3.1.1. A properly executed Record Request is received showing the requesting party's name, address, phone and fax number;

3.1.2. The identity of the requesting party is confirmed by return call to the phone number on the Record Request as well as by calling the client directly;

3.1.3. The signature on the Record Request is no older than six months prior;

3.1.4. The Request is accompanied by a copy of the client's signed photo ID which matches client signature on the blood test consent form.

4. **Records Retention.**

4.1. The Records Retention Schedule for confidential information consists of only an active period of the record.

4.2. The Information Custodian maintains a written inventory of records and file locations.

4.3. There are 2 types of confidential records addressed under this Retention Schedule:

4.3.1.Confidential information relating to general client services which includes: contact sheets; client correspondence; client satisfaction and health outcomes surveys. Retention for general client services is more than 6 months but less than 12 months after first contact with the client.

4.3.2.Confidential information specific to HCV and HIV counseling, consent and testing include: study data; risk assessments; informed consent forms; laboratory forms and test results. Retention for HCV and HIV counseling, consent and testing information is 7 years after the specimen collection date or beyond if needed for project audits or until findings resolved. Certain records by Memo of Agreement or Contract, may be retained for a longer duration identified by Contract. The Executive Director consults with the Security Coordinator to identify these records.

4.4. Records reaching the end of the retention cycle are destroyed annually at a date established by the Security Coordinator and/or the Executive Director.

E. ELECTRONIC SECURITY

1. **Electronic File Quality Assurance.**
   - 1.1. The Security Coordinator and/or the Executive Director are responsible for all electronic confidential files.
   - 1.2. Management of confidential electronic files is implemented by the Executive Director and monitored periodically by the Security Coordinator to ensure compliance with policy, protocol and procedures.

2. **Computer Locations.**
   - 2.1. Computers with confidential information are located secured areas which limit access to authorized individuals.
   - 2.2. The network server is located in a Secure Computer Room.

3. **Computer Password Protection.**
   - 3.1. Computers with access to confidential information are password-protected:
     - 3.1.1. Windows login passwords are a minimum of 8 characters in length and expire every thirty days;
     - 3.1.2. Workstation (screensaver) passwords are unique for each staff person and are a minimum of 8 characters in length; and
     - 3.1.3. Open Database, Read, Insert, Copy and/or Delete privileges for the proprietary software (HIMS™) are assigned through both workgroup and individual usernames and passwords.

4. **Network Connection.**
   - 4.1. Computers with access to confidential information are stored on the local area network (LAN) with the following safeguards:
     - 4.1.1. Confidential information is stored in a manner that prevents users from unauthorized access;
     - 4.1.2. Removable media (A drive) is either disabled or locked on all workstations to prevent unauthorized copying of confidential information onto a diskette. CD drives are Read Only.
     - 4.1.3. Users are restricted to specific workstations; and
     - 4.1.4. Time of day timer is used to control hours of access to the network.

5. **Anti-Virus procedures.**
   - 5.1. All reasonable measures are taken to prevent, detect, remove, and report viruses. Users are informed about the procedures for detecting viruses and limiting the spread of infection.
   - 5.2. McAfee Online virus scanning tool runs at all times and is used to remove a virus from an infected file, program, or storage media. All computers maintain up-to-date virus definitions.

5.2.1. The McAfee Online virus definitions is updated by each employee on their assigned computer every time an update notice appears on the desktop. The Security Coordinator updates the virus definitions on the network server.

5.2.2. Employees perform a McAfee Anti-Virus system scan at least once a week on their respective computers. The Security Coordinator performs the McAfee Anti-Virus system scan at least once a week on the network server.

5.2.3. Virus scanning results are checked by appropriate staff.

5.3. NO email attachment is ever opened without first confirming the source of the email and the attachment by sending a return email requesting such verification. These attachments are deleted immediately, then "double deleted" by emptying the Trash.

5.4. NO external program(s) may be installed/added to any computer unless first approved in writing by the Executive Director. When approved, all software and data imported is scanned before the file is opened and read by the user.

5.5. NO email newsgroup or listserv subscriptions are made by employees unless first approved in writing by the Executive Director.

5.6. Any employee who suspects that a computer is infected with a virus informs their supervisor or other designated staff and immediately disconnects the suspect computer from the network physically by removing the gray cable from the back of the computer.

5.6.1. The employee and/or supervisor runs a full anti-virus system scan. When informed that a virus has been detected and is likely to be widespread, the designated personnel shall inform all users who may have been exposed to the same programs or data that a virus may have infected their systems.

5.6.2. Any machine thought to be infected by an unknown virus with no known cleaning routine available, is immediately isolated with appropriate measures taken to remove the virus. If necessary, the machine should be disconnected from all networks.

5.6.3. If McAfee scanning tools still do not remove the virus and McAfee cannot provide an update in a satisfactory time-frame, that computer remains off network and unused until such time that an update is received and the computer can be properly cleaned.

5.7. All the steps taken to recover from a virus infection incident are documented. These steps are useful as a future reference in updating procedures and educating personnel.

6. Internet / Email Connection.

6.1. Computers with access to confidential information have internet connectivity with the following safeguards:

6.1.1. DSL internet connection is terminated when not in use.

6.1.2. A dedicated telephone line is used for DSL access.

6.1.3. Not applicable to the Department of Health Policy:

6.1.3.1.DSL does not have dial back capabilities to enable.

6.1.3.2.DSL does not have caller list functions to activate.

6.2. Configuration of staff email permits incoming, but not outgoing electronic mail to prevent unauthorized emailing of confidential client information.

7. Encrypting Electronic Data.

7.1. Electronic data files containing confidential information are encrypted.

7.2. This applies to all files electronically transmitted or transported in any way, including those on a Laptop Computer. Single file encryption/decryption is achieved with HidePro®.

8. Securing External Media.

8.1. Data backups are locked in a secured area with access limited to authorized individuals only.

8.2. Diskettes containing confidential information are secured in a locked file cabinet at the end of the day.

8.3. External backup drives are affixed to an immovable object with a Security Cable when in use and/or maintained in a locked file cabinet.

8.4. The Security Coordinator is responsible for rotating external backups nightly. External backup drives are removed from the office in a fireproof lock-box.

9. Notification of Laptop Use.

9.1. The HIV Testing Director or Executive Director notifies the Miami-Dade County Health Department of the use of laptops for confidential information.

10. Securing Laptops Offsite.

10.1. When offsite, a laptop computer is secured either in the locking catalog case and safeguarded at all times or secured to an immovable object using a Kensington Security Cable and Sonic Motion Alarm.

10.2. When staff leave a temporary workstation (even for a moment), the laptop remains secured to an immovable object using the Kensington Security Cable and the office door is locked on exit. If there is no door lock, the laptop is placed in the locking catalog case affixed with the Sonic Motion Alarm.

10.3. Staff takes reasonable and prudent care to safeguard both the laptop and information, including removing it from their vehicles and maintaining it in their home overnight.

11. Securing Laptops In The Office.

11.1. The Security Coordinator runs a full virus scan before connecting a laptop to the local area network (LAN), then establishes the connection the LAN and synchronizes the replica and the master file.

11.2. The laptop functions as a regular workstation on the LAN while in the office. Laptops are secured to the desktop of the workstation using a Kensington Security Cable.

11.3. When staff leave a laptop workstation (even for a moment), they lock their office door on exit.

F. COMPLIANCE PROCEDURES

1. Compliance Quality Assurance.

1.1. The Information Security Coordinator conducts a compliance check-up each month to ensure compliance with confidentiality and security policies, protocols and procedures.

1.2. The Information Security Coordinator writes a Compliance Report for review by the HIV Testing Director and Executive Director.

1.3. Information and Workplace Safety Meetings are conducted quarterly or more frequently if needed.

2. Corrective Action.

2.1. The corrective action plan includes a copy of the completed Department of Health security information risk assessment form or confidentiality and security incident report.

2.2. Corrective action steps identified during routine compliance audits of a confidentiality or security incident are documented on Department of Health Confidentiality and Security Incident Reporting form (DH 1139).

2.3. Corrective action plans are developed in a manner, which clearly identifies the finding, the steps required to correct the situation, the expected date of completion, and the individual(s) responsible for implementing and monitoring the action item.

2.4. Corrective action plans are discussed with the individual(s) who have the responsibility or authority to make recommendations for improvement, implement corrective actions and monitor corrective action steps.

2.5. Operating procedures are updated, where appropriate, to reflect changes as a result of the corrective action plan.

2.6. Company-wide retraining is provided for areas needing improvement.

2.7. Corrective action for employee breeches of information security policy and procedures relating to HIV and/or HCV counseling and testing information may include:

2.7.1. 1st offense, verbal warning with documented retraining and repeat demonstration;

2.7.2. 2nd offense, written warning, documented retraining and 90-day probation; and

2.7.3. 3rd offense, suspension without pay or termination.

3. Employee Confirmation

3.1. I have received, read and had any questions I may have had, answered to my satisfaction. I understand my responsibilities and agree to abide to the procedures outlined in this policy. I also understand that I am required to report any breeches of security or concerns about policy, procedure or protocol immediately to my supervisor, the Security Coordinator or the Executive Director.

____________________________ ________________________

Employee Signature Date

____

Employee Name