HEP-C ALERT, INC.

INFORMATION SECURITY RISK ASSESSMENT & CORRECTIVE ACTION PLAN

Initial Audit Date: 10/18/02

SECURITY 1 – INFORMATION SECURITY POLICIES, PROTOCOLS AND PROCEDURES			
1.	The Information Security Policies, Protocols and Procedures are accessible to all staff. List the location in the comments section.		1 copy of the policies and protocols is located in the Administrative Assistant's office and 1 copy is located in the Executive Director's office.
2.	Monitoring takes place at least annually to assess compliance with the Information Security Policies, Protocols and Procedures.		Monitoring takes place monthly by the Security Coordinator. Audit forms are maintained in the Administrative Assistant's office.
3.	Supplemental operating procedures have been developed.		General Information Security Policy.
4.	Supplemental operating procedures are updated at least annually, or when appropriate as a result of a corrective action plan or policy revisions.		
5.	The most recent version of the supplemental operating procedures has been filed with the DOH Security Coordinator. If no, attach the most recent version to this assessment.		
6.	Supplemental operating procedures are accessible to all staff. List the location in the comment section.		Located as indicated in 1.1.
SECURITY 2 – DESIGNATION OF SECURITY COORDINATOR			
7.	List the name of the security coordinator in the comment section.		Elliott Kim.
8.	Security coordinator delegation is documented in the security coordinator's personnel file.		Yes.
9.	Security coordinator responsibilities have been included in the security coordinator's position description.		Position responsibilities are in the personnel file.
10.	Security coordinator responsibilities are consistent with those stated in Security 2.V. (If not please indicate the item number)		Yes.
SECURITY 3 – DESIGNATION OF INFORMATION CUSTODIANS			
11.	List all information custodians, their corresponding information sets, and individuals with authorized access to these information sets either in the comments section or as an attachment to this assessment.		LaShawn Mears.
12.	All information custodians have a signed Delegation of Authority (DH Form 1151) in their personnel file.		Yes.
13.	Information custodian responsibilities have been included in position descriptions for all custodians.		Position responsibilities are in the personnel file.
14.	Information custodian responsibilities are consistent with those listed in Security 3.V. (If not please indicate the item number)		Yes.
SECURITY 4 – RETENTION OF RECORDS			
15.	List the name of the records retention liaison who ensures that all local records are retained according to the Records Retention Schedule, or beyond the scheduled retention date in special circumstances.		LaShawn Mears.
16.	The records retention liaison has a copy of the Department of State, Division of Library and Information Services, Bureau of Archives and Records Management storage and disposition procedures.		Yes.
SECURITY 5 – ARCHIVING AND DISPOSITION OF RECORDS			
17.	Records are archived and disposed according to the Department of State, Division of Library and Information Services, Bureau of Archives and Records Management storage and disposition procedures.		Yes. Records have an active period only.
18.	All confidential records are archived and disposed of in such a way as to ensure that confidentiality and security are maintained.		Yes.
19.	Confidential information that requires shredding, including STD, HIV/AIDS and TB case reporting information, is shredded within the secured area.		Yes.
20.	List the types of confidential records and the method of archiving or disposition performed since the last risk assessment, either in the comments section or as an		See General Information Security Policy #D4. 2 types of records: 1) General information relating to client services

	attachment. (Examples are shredding, incinerating, archiving in a secured facility.)		including correspondence, satisfaction surveys, contact records; and 2) Testing information including consent, survey, and test results. Type 1 records are retained between 6 and 12 months; Type 2 records are retained 7 years. Disposition: American Document Destruction bin located in Secure Area.
SECURITY 6 , SECURITY 16, SECURITY 18 – MAINTAINING SECURED AREAS FOR CONFIDENTIAL INFORMATION, INCLUDING HIV/AIDS, STD AND TB CASE REPORTING			
21.	All confidential information is maintained in a secured area to ensure that client or employee confidentiality is safeguarded, and data integrity is protected.		Yes.
22.	A reliable locking system including a deadbolt lock has been installed to prevent unauthorized access to the secured area. List the type of locking system(s) for all designated secured areas in the comment section, or as an attachment.		Yes. Locking file cabinet with padlocked bar; door handle lock and combination Simplex deadbolt lock.
23.	Secured areas with street-level, window access have measures in place to prevent unauthorized access via windows. List the preventive measures for all secured areas that meet this criteria, either in the comments section or as an attachment.		Not applicable.
24.	Secured areas without solid ceilings (i.e., drop ceilings) have measures in place to prevent unauthorized access via ceilings. List the preventive measures for all secured areas that meet this criteria, either in the comments section or as an attachment.		Locking file cabinet with padlocked bar; door handle lock and combination Simplex deadbolt lock. Motion detector located in rear hallway and front reception area and front office(s). No other measures at this time.
25.	Secured areas limit access to a documented list of authorized personnel.		Yes.
26.	A key custodian and an alternate key custodian have been designated for each secured area. List the name(s) of key custodians and alternates for each secured area in the comment section or as an attachment.		Elliott Kim, La Shawn Mears.
27.	Key custodians maintain control of keys to the secured area, and provide keys to authorized employees.		Yes.
28.	Authorized visitors to the secured area sign in and out on an access log that includes their signature, time in and out, purpose for visit, items taken from the secured area.		Yes.
29.	The key custodian or alternate reviews the access log at least monthly, signs and dates the last entry of record.		Yes.
30.	An inventory of equipment and information located in the secured area(s) is documented at least annually.		Yes.
31.	Visitors to the secured area without authorized access are escorted to and from their destination.		Yes.
32.	HIV/AIDS, STD and TB case reporting information, either computerized or hard copy, is located in a secured area(s).		Yes.
33.	Main or central computer control room(s) are designated secured area(s) and meet the requirements of a secured area.		File server relocated to a room with a locking door. **
34.	Each case reporting area has a shredder available so that confidential information is not removed from the secured area to be shredded.		Office uses a central document destruction bin. Information is transported to/from offices to the bin in folders.
35.	Procedures for removing confidential information from the secured area(s) are documented and monitored to ensure compliance.		Yes.
SECURITY 7, SECURITY 16 AND SECURITY 18 – MAINTAINING CONFIDENTIAL INFORMATION INCLUDING HIV/AIDS, STD, TB CASE REPORTING			
	Maintaining Confidential Information in the Clinic. Complete Lines 36-43 For Clinic Settings Only.		
36.	Specialty clinics, such as STD, HIV/AIDS and TB, are labeled in such a way as to protect client confidentiality.		N/A.
37.	Sign-in logs in general clinics only collect the time of arrive and the client's name. STD, HIV/AIDS and TB clinics do not		Yes.

	use sign-in logs.		
38.	Client names are not called in the waiting rooms of STD, HIV/AIDS and TB clinics. List the procedure for client callbacks in the comment section.		Yes.
39.	Telephones are answered in such a way that does not identify a specialty clinic.		Yes.
40.	Client registration, interviews and counseling takes place in areas where confidential information cannot be overheard.		Yes.
41.	Billing, appointment scheduling and reminder procedures are performed in such a way that client confidentiality is not compromised.		Yes.
42.	Medical records do not show confidential information on the outside, except for medication allergies or name alert.		Yes.
43.	Medical records are not segregated or identified by disease when filed.		Yes.
	Maintaining Confidential Information – All Settings		
44.	Confidential information, including HIV/AIDS, STD and TB case reporting information, is locked in a file cabinet or file drawer within the secured area when not in use.		Yes.
45.	Confidential information, including HIV/AIDS, STD and TB case reporting information, has not been found to be left unattended or unsecured since the last risk assessment.		Yes.
46.	Staff has not been overheard discussing confidential information in public settings since the last risk assessment.		Yes.
47.	HIV/AIDS case reporting information is time stamped upon receipt and disposition within 90 days of receipt.		Yes.
48.	HIV/AIDS, STD and TB line lists are not removed from the secured area except to send to case reporting staff at the county health departments.		N/A.
	Maintaining Computerized Confidential Information – All Settings		
49.	Computer monitors that routinely display confidential information are not visible to unauthorized persons.		Yes.
50.	Procedures for assigning and maintaining computer user identifications are documented in the supplemental operating procedures.		Yes.
51.	Computers maintaining confidential information, including case report information, are password protected, using passwords at least 8 characters in length and require changing every 30 days.		Yes.
52.	There have been no documented incidents of employees sharing passwords or otherwise disclosing a password since the last risk assessment.		Yes.
53.	Virus protection software has been installed and regularly updated for all computers.		Yes.
54.	Local procedures have been developed and disseminated in the event a computer is suspected of being infected.		Yes.
55.	All external data files to be transported or transmitted are encrypted. List the encryption software used in the comment section.		Yes. HidePro® used for individual files. DiskCrypt® will be purchased by 10/31 for server and backup drives.
56.	Disk drives on computers that contain confidential information provide a method to restrict the downloading of information onto a disk (i.e., locking disk drive or removable disk drives). List the method(s) of restriction in the comment section or as an attachment.		Yes. Floppy drives on staff workstations are disabled at the boot level. CD Rom drives on all PCs are Read Only. Floppy drives on E.D., Admin Assistant, and Network Server are locked.
57.	Confidential data back-up disks or tapes are encrypted and stored in locked storage within a secured area.		Yes. HidePro® used for individual files. DiskCrypt® will be purchased by 10/31 for server and backup drives.
58.	Printers connected to computers that contain confidential information are located in a secured area.		**No.** Printer is not in a secure area. See General Information Security Policy #C3.
59.	Reports and files generated from computerized databases are logged, tracked and reviewed by a designated person(s). List the person(s) in the comment section or as an attachment.		Yes.

60.	List the name of the designated person(s) who is responsible for the electronic file transmission of case reporting information in the comment section or as an attachment.		N/A.
61.	Computers with HIV/AIDS, STD and TB case reporting information, which also have modem connectivity, meet the four standards listed below: • External modems are turned off when not in use; • Dial back capabilities are enabled; • Modem caller list functions are activated; • Dedicated phone lines are used for modem access.		Yes. See General Information Security Policy #E5.
62.	Computers with HIV/AIDS, STD and TB case reporting information, which also have wide area network connectivity, meet the three standards listed below: • Confidential information is not stored in directories with unlimited access; • User account logons are limited to specific workstations; • User access is limited by hours of access.		Yes. See General Information Security Policy #E2 - E4.
63.	Network configurations do not allow unauthorized access to network drives that store confidential information or databases requiring data integrity assurances.		Yes.
64.	Laptop computers used to store confidential information are password protected and data are encrypted.		Yes.
65.	Laptop computers are not used to collect HIV/AIDS, STD and TB client identifying information.		Pending approval.
	Telephone and Fax Procedures – All Settings		
66.	Staff has not been overheard discussing confidential information, including HIV/AIDS, STD and TB case reporting information, by phone in areas where unauthorized persons can hear the conversation.		Yes.
67.	Fax machines that transmit or receive confidential information are located in secured areas.		No. No faxing of HIV information is permitted. See General Information Security Policy #B5
68.	A cover sheet marked “Confidential” accompanies all confidential faxes, which includes the language required in Security 7.1.V.		Yes for Confidential. N/A for HIV.
69.	Staff has been trained to confirm by phone that confidential information was faxed to the correct destination.		Yes for Confidential. N/A for HIV.
70.	Staff has been trained to confirm that the client has signed a release of information prior to faxing, and there have been no unauthorized faxes documented since the last assessment.		Yes for Confidential. N/A for HIV.
71.	A notation is made in the client or employee record identifying the information that was faxed. This notation is signed and dated by the person who faxed the information.		Yes for Confidential. N/A for HIV.
72.	Staff has been trained that HIV/AIDS information is not to be faxed, and there have been no unauthorized faxes documented since the last assessment.		Yes.
	Mailing Confidential Information – All Settings		
73.	A secured mail intake site is used to receive incoming confidential information. List the secured intake site(s) in the comment section, or as an attachment.		Yes. Security Coordinator Office.
74.	Mailrooms and mailboxes prevent unauthorized access to incoming and outgoing mail.		Yes.
75.	Outgoing confidential mail is double enveloped.		Yes.
76.	Outgoing HIV/AIDS, STD and TB case reporting information is double enveloped and sent by traceable mail.		Yes.
	Maintaining Confidential Information in the Field- All Settings		
77.	Confidential information is transported into the field only by those employees who are required to in order to perform their jobs. Position numbers of these employees are documented in the supplemental operating procedures.		Yes.
78.	HIV/AIDS, STD and TB worklists do not include titles or headers that identify the type of list or clients.		Yes.

79.	Confidential information, including case reporting worklists, with client identifiers only contain one day's workload and are kept with the employee at all times when outside of the secured area.		Yes. Exception - two day workload for ARHIP counselors.
80.	Confidential information, including case reporting worklists, are limited to only the descriptive information needed to perform job responsibilities.		Yes.
81.	A log is kept to track confidential information leaving the secured area that includes date and time out, type of information, employee taking information, reason, date and time in.		Yes.
82.	Confidential information, including HIV/AIDS, STD and TB case reporting information, must be returned to the secured area by the end of the working day unless the appropriate approval (i.e., supervisory staff) has been obtained and documented.		Yes. Exception - two day workload for ARHIP counselors. All other cases by E.D. approval.
83.	Laptop computers with confidential information (except HIV/AIDS, STD and TB information which cannot be kept on laptops) is not kept at an employee's home and is returned to the secured area at the end of the day.		Yes. Exception - two day workload for ARHIP counselors. All other cases by E.D. approval.
	Maintaining Confidentiality During Disease Intervention Investigations – Answer Lines 84-87 for STD Staff Only		
84.	Only the hard copy (green or computer generated) of the STD Field Record (CDC Form 73.2936S) is taken into the field.		N/A.
85.	The results of field activity are documented on the back of the record. Documentation does not name the disease or reference sensitive information (i.e., risk exposure, names of partners, etc.).		N/A.
86.	Copies of HIV/STD laboratory results are not taken into the field with the exceptions listed below, • Transferring results to a satellite clinic; • Prearranged posttest counseling in an institutional setting or other setting where several clients will receive posttest counseling. There have been no documented incidents of HIV/STD laboratory results being taken into unauthorized locations since the last risk assessment.		N/A.
87.	When transporting HIV/STD laboratory results to authorized locations, the results are in the possession of the employee at all times. There have been no documented incidents of results being left unattended since the last risk assessment.		N/A.
SECURITY 8 AND SECURITY 9 – INFORMATION SECURITY RISK ASSESSMENT AND INCIDENT REPORTING			
88.	A risk assessment has been performed at least annually and filed with the DOH Security Coordinator.		N/A. First assessment.
89.	All items listed as "not in place" include a corrective action plan with corrective action steps, person responsible for each step and due date for each step.		N/A. First assessment.
90.	Incident reporting procedures are followed and documented. List the number of documented incidents since the last risk assessment in the comment section.		N/A. First assessment.
91.	Incident reports and corrective action plans are maintained by the security coordinator consistent with procedures for storing confidential information.		N/A. First assessment.
SECURITY 10 AND SECURITY 18– CONTINGENCY PLANNING, INCLUDING DATA AND SOFTWARE BACK-UP			
92.	List the name of the contingency plan coordinator in the comment section.		Alex Baird.
93.	The contingency plan includes written operating procedures for the back up, storage and retrieval of electronically stored data and other valuable or critical computer systems in the event of a disaster.		Yes.
94.	The contingency plan includes written operating procedures for securing confidential information in the event of a disaster.		Yes.

95.	Two sets of computer back-up storage media are used in rotation. The most recent storage media is stored off-site.		Yes.
96.	The systems administrator has a back-up copy of all software programs, including modifications and updates.		Yes.
97.	Fire detection/suppression, power conditioning and other protections systems are in place to assure continued service of critical computer systems.		Yes. UPS support, surge protectors and fire extinguishers.
98.	Preventive maintenance is performed regularly on all computers and communications systems.		Yes.
99.	The contingency plan is tested at least annually.		Yes.
SECURITY 11 AND PERSONNEL – CONFIDENTIALITY STATEMENT OF UNDERSTANDING AND BACKGROUND SCREENING			
100.	Staff who review and utilize confidential information are designated as "sensitive" positions, and are background screened as a condition of employment. List the number of designated sensitive positions in the comment section.		No.
101.	Students, post-graduate trainees and volunteers who review and utilize confidential information are designated "sensitive" and are background screened. List the number of students, post-graduate trainees and volunteers in the comment section.		No.
102.	Sensitive position personnel files have been reviewed for documentation of initial FBI and FDLE background screening.		No.
103.	Sensitive position personnel files have been reviewed for documentation of periodic FDLE background screening (at a minimum, five years since initial background screen).		No.
104.	All employees and volunteers have signed the Confidentiality and Security Statement of Understanding Section A (DH Form 1120).		Yes.
105.	All employees and volunteers who have access to computer related materials have signed the Confidentiality and Security Statement of Understanding Section B.		Yes.
106.	All employees have signed an acknowledgement of receipt of the Department of Health Personnel Handbook.		N/A.
107.	Staff has been informed of consequences related to non-compliance and of potential disciplinary actions and criminal penalties during Level 1 Training.		Yes.
SECURITY 12 – ASSURING SECURITY AND CONFIDENTIALITY PRACTICES WITH CONTRACT PROVIDERS			
108.	All contracts where the contract provider has access to confidential or sensitive information include the security and confidentiality provision language, version July 14, 1998. Contract providers have been given a complete and current edition of the Department of Health Information Security Policy.		N/A.
109.	The contract manager to assure information security and confidentiality requirements are in compliance monitors contract providers at least annually.		N/A.
SECURITY 13 – CORE SECURITY AWARENESS TRAINING			
110.	List the name of the training coordinator in the comment section.		Angel Acevedo: MDCHD.
111.	Level 1 training is provided to employees within 30 days of employment and is consistent with the standards listed in Security 13.V. List the method of training in the comment section (group course, self-study, individual training, etc.).		Yes. New staff will be trained by MDCHD.
112.	Documentation of Level 1 training is maintained for each employee either in personnel files or through the Training Direct tracking system.		Yes.
113.	Annual update training is provided to all employees. Documentation is maintained for each employee either in personnel files or through the Training Direct tracking system.		Yes.
SECURITY 14, SECURITY 15 AND SECURITY 17– RELEASE OF CONFIDENTIAL INFORMATION, INCLUDING HIV TEST RESULTS AND HIV/AIDS CASE REGISTRY DATA			

114.	Local procedures for releasing confidential information within the health department, to a requesting patient, to third-party payers, for legal requests, for HIV test results and for immunization information are documented in the supplemental operating procedures.		Yes.
115.	Local procedures are consistent with guidelines in Security 14 and Security 15.		Yes.
116.	There have been no documented incidents of releasing confidential patient information without authorization since the last risk assessment.		Yes.
117.	Local procedures for releasing HIV/AIDS case registry data are documented in the supplemental operating procedures and are consistent with Security 17.		Yes.