I. Introduction

The states’ HIV/AIDS surveillance systems are responsible for sustaining the success of the standards of the Centers for Disease Control and Prevention (CDC) surveillance security model. State and local health department staff, health care providers, and the affected community must ensure that the data are complete, timely, representative, and useful for public health planning and prevention activities. Effective surveillance can “(1) act as an early warning system by detecting new trends and patterns in the epidemic; (2) focus resources and interventions where most needed; (3) promote behavioral and environmental changes by identifying modes of exposure and educating populations that are at risk; (4) evaluate the efficacy of intervention efforts; and (5) influence legislation and social change by informing policymakers and citizens about the epidemic,” (CDC Security Standards, 10/30/97), and (6) identify infected persons so treatment can be provided as early as possible when it may be most effective.

Kentucky’s HIV/AIDS surveillance success depends on the trust and cooperation of the public and their health care providers. The Commonwealth of Kentucky has statutes to protect individuals against HIV/AIDS discrimination (KRS 207.135, 207.150, 207.160, 207.250, 207.260, 304.12013). The HIV/AIDS Program also administers the Professional and Public Education Program required by Kentucky statutes which were established to educate employers, educators, law enforcement, health and medical providers and other professionals in dealing with the disease and attitudes that may be associated with it (KRS 214.600, 214.605, 214.610, 214.615, 214.620, and various Administrative Regulatory requirements for certification and licensure of professional specialties). However, there are no guarantees regarding attitude, and consequences could be devastating if sensitive information about high risk behaviors or HIV status reaches employers, insurers, schools, family or acquaintances. This may cause many persons at risk for HIV/AIDS to avoid testing and treatment. Because of these concerns, as well as changing technologies in surveillance systems, both the CDC and the Kentucky HIV/AIDS Program are aware of the need to develop comprehensive, detailed security guidelines in attempts to provide data for maximum public health utility with an absolute minimum risk of disclosure. The security policy detailed below describes that effort, with standards for: (1) physical security, (2) electronic security, and (3) operational security. Also included are sections for security violations and quality control measures.

In 1982 Kentucky enacted state legislation requiring the reporting of AIDS cases. In 1989 Kentucky enacted regulations requiring the reporting of HIV cases by a ‘Unique Identifier’, consisting of the person’s initials of last and first name, date of birth, and last four digits of the Social Security number. As of July 13, 2004 based on 902 KAR 2:020, Section 7, Kentucky requires HIV to be reported by Name, along with Sex, Race/Ethnicity, Risk Factor, as identified by CDC, County of Residence, Name of Facility submitting report, Date and Type of HIV Test performed, results of CD4+ cell count and CD4+% results, of Viral Load testing in 902 KAR 2:020, Section 7.
HIV/AIDS SURVEILLANCE SECURITY & CONFIDENTIALITY POLICY

HIV and AIDS cases are reported to only two sites throughout Kentucky, the Louisville Metro Health Department and the Kentucky Department for Public Health in Frankfort. 902 KAR 2:020, Section 7(2)(a) states that reports for residents of Jefferson, Henry, Oldham, Bullitt, Shelby, Spencer, and Trimble Counties shall be submitted to the HIV/AIDS Surveillance Program of the Louisville Metro Health Department (i.e., satellite office). Cases from all other Kentucky counties of residence are reported to the Kentucky HIV/AIDS Program in Frankfort (i.e., central office).

II. Physical Security

A. Security of Location

The following descriptions apply to both the central and satellite office, unless otherwise noted. Access to the HIV/AIDS surveillance offices and equipment, including hard copy files containing identifying patient data, shall be restricted to HIV/AIDS surveillance staff unless specifically authorized by the HIV/AIDS Surveillance Coordinator. Access to any secured area that contains surveillance data or can be used to access surveillance data by unauthorized individuals can only be allowed when authorized surveillance or IT personnel are present, with the exception of the eHARS, SCAN and HAN server locations. For these locations, although physical access is possible for unauthorized IT personnel, login access to the servers is restricted to authorized IT personnel. See Section IV. Operational Security and Data Access.

The surveillance office doors have two locks, a deadbolt lock as well as a regular lock. The doors to these offices shall be kept locked at all times. Bomb- and fire-proof lockable file cabinets, with an additional bolting system on the outside of each, are used to store written materials and back-up disks of the HIV/AIDS databases. When the project office is unattended, files, laboratory reports, case reports, diskettes, disk back-ups and any other materials which contain identifying information on HIV/AIDS cases will be closed and placed in the above described file cabinets, which are then double-locked.

The HIV/AIDS Surveillance Coordinator, Surveillance Technician, and Epidemiologist keep the original keys to the central office, and the HIV/AIDS Branch Manager keeps duplicate keys for use on an emergency basis only. Emergency basis is defined as the absence of the Surveillance Coordinator, Technician and Epidemiologist, and public health protection is required. Only the HIV/AIDS Surveillance Coordinator and Surveillance Technician, and Epidemiologist have keys to the file cabinets. The HIV/AIDS Surveillance Nurse Consultant shall keep the satellite office and file cabinet keys. The immediate supervisor of the Surveillance Nurse Consultant shall maintain duplicate office keys, to be utilized only on an emergency basis. Emergency basis is defined as absence of the Surveillance Nurse Consultant, and public health protection is required.

The central surveillance office is located on the second floor. The windows cannot be opened, and are covered with blinds. The office shall be arranged in such a way as to prevent long-distance visual access to the computer screens and documents. The satellite office is arranged in a similar fashion.

The Surveillance Coordinator, Surveillance Technician and Surveillance Nurse Consultant maintain the case registries by using the CDC enhanced HIV/AIDS Reporting System (eHARS) database. Data are collected through both hard case reports, telephone and chart reviews and are entered electronically into eHARS.
B. Receipt of Confidential Information

Incoming Mail
Incoming mail is delivered to the HIV/AIDS Branch mail stop. The mail is sorted and placed in the Surveillance Coordinator’s mailbox. Mail is removed from the mailbox before the close of business each day. Only HIV/AIDS surveillance staff shall open incoming confidential surveillance mail. If other staff within the Kentucky Department for Public Health (KDPH) receives mail intended for the HIV/AIDS Surveillance Program, the mail shall be hand delivered unopened to the surveillance staff, or placed under the surveillance office door. When mail meant for the Surveillance Program is received with incorrect address information, surveillance staff will contact the mailer and advise him/her of the correct address information. Mail addressed to the surveillance staff opened by other staff within KDPH shall be considered a security breach (See Section V. Security Violations).

Outgoing Mail
All outgoing mail containing confidential information must be double enveloped, and stamped “Confidential, to be opened by addressee only.” The inner envelope shall also be marked, “Please mail if found,” and include the HIV/AIDS Surveillance program address. There will be no mention of HIV or AIDS on the envelopes.

When possible, confidential information exchanged between the satellite and central offices shall be carried in a locked briefcase. Insured and traceable overnight mail (i.e., Federal Express) shall be used between the satellite and central offices in all other circumstances. All confidential material must be placed in an envelope with the HIV/AIDS Surveillance program address, before placing within the Federal Express Mailer. A single mailing shall not include information identifying more than 50 names. Transmission of information with more than 50 names shall be divided into multiple mailings. Before sending confidential information between sites, the surveillance staff will contact the other office to notify of the mailing. The other office will confirm the mailing was received via telephone.

When HIV/AIDS cases reported to the Surveillance Program are residents of other states, the case reports shall be mailed to the authorized HIV/AIDS surveillance personnel for the other state. The CSTE listing of authorized surveillance personnel shall be utilized to verify contact information. The information shall be mailed using double envelopes, with both envelopes stamped “Confidential, to be opened by addressee only.” The inner envelope shall also be marked, “Please mail if found,” and include the other state’s HIV/AIDS Surveillance Program address. Out-of-state surveillance personnel shall be notified via telephone before confidential information is sent.

Written receipt of confidential information via mail from another state’s surveillance program shall be conducted the same way as the paragraph immediately above, using two different envelopes to mail reports addressed to a specific HIV/AIDS surveillance staff person. Phone confirmation of written materials is recommended over mail confirmation.

Telephone
There are two phone numbers dedicated to the HIV/AIDS Surveillance Program. These phone numbers shall be referenced in all information regarding HIV/AIDS reporting. These direct numbers limit potential security breaches. If staff outside of the Surveillance Program receives a call about HIV/AIDS reporting, they must tell the caller that they are not authorized to take
messages that include any identifying information, and then transfer the call to the HIV/AIDS surveillance staff.

The HIV/AIDS Surveillance Program telephone voice mail shall not be used to report cases, nor is case information reported to other states or reporting sites to be left on their voice mail. The office’s voicemail shall clearly state that no personal identifying information should be left on the voicemail.

The following policies shall be followed when out-of-state surveillance personnel contact the Kentucky HIV/AIDS Surveillance Program requesting confidential information. If the out-of-state surveillance contact is unfamiliar to the surveillance staff, the caller is told he/she will receive a call back with the information requested. The Kentucky staff must then review the CSTE listing of authorized surveillance personnel by state, and if on the list, the contact person shall be called back with the information. If not on the CSTE list, Kentucky’s CDC Consultant shall be contacted for confirmation prior to calling the contact back with the requested information. If the out-of-state surveillance contact is familiar to the Kentucky staff (i.e., recognize the contact’s voice due to many routine interactions), the Kentucky staff can provide the information requested immediately, without calling back to confirm the individual’s identity. See Section IV. Operational Security and Data Access, Part B. Data Release, for more information on the data that may be released to out-of-state surveillance personnel.

Infection Control Practitioners and physicians may call the HIV/AIDS Surveillance Program to report a case, but HIV/AIDS surveillance personnel shall not confirm or deny whether the case has been previously reported. Surveillance staff shall check the case information against the current records and eliminate duplicates, and shall call back if there are additional questions. Surveillance staff shall not release any information to providers, except for in the circumstance listed in Section IV. Operational Security and Data Access, Part B. Data Release.

**Faxes/E-mails**
NOT IN USE August 2014: Confidential information may be transmitted by fax. A fax line is physically residing within the central surveillance office. A code must be used to retrieve the fax. This code is not to be shared with anyone outside of the surveillance office.

Confidential information may be transmitted via email using an encrypted program. Before using, the program(s) in question will be reviewed by the Chief Security Officer for clearance. This type of email program requires user accounts to be established and is password/security phrase protected.

If confidential information is received via non-encrypted email, inform the surveillance coordinator immediately. Delete the email from the inbox. Then, delete it from the deleted items folder.

Confidential emails must not be accessed on personal phones. If the ky.gov email account is synced to a personal smartphone and a confidential email is received and accessed mistakenly, ensure that the email is not in your phone inbox or downloads before you leave the surveillance office. Follow the same procedure for deleting the email and notify the surveillance coordinator.

COT backs up email for 14 days then it is permanently deleted.
All documents containing confidential information shall be shredded before disposing of them. The shredder, located in the surveillance program office, shall be of commercial quality with a crosscutting feature. See Section IV. Operational Security and Data Access, Part C. Record Retention Policies.

C. Offsite Data Security

HIV/AIDS surveillance staff shall travel with confidential information only to perform site visits or other necessary surveillance job functions. Confidential information shall be transported in a locked briefcase. These materials shall be returned to the office for lockup by the end of each business day. HIV/AIDS surveillance staff shall be prohibited from taking confidential materials home unless a prolonged site visit prevents them from returning to the office. In this case, the information shall remain in a locked briefcase in possession of the surveillance staff member until it can be returned to the office for secure storage. Also in this situation, permission must be granted and documented by the Surveillance Coordinator before taking confidential materials home.

If traveling by car, the briefcase shall be locked within the trunk during travel. The briefcase should not be left unattended in locked cars. In vehicles without a lockable trunk, the briefcase shall be stored out of sight and in a location where movement is limited, such as under a seat, or within a storage container.

Any line list, in either hard copy or electronic format, taken outside of the surveillance office shall not contain any title or other information that associates the document with HIV/AIDS.

While working off-site, all confidential materials must remain in the possession of HIV/AIDS surveillance staff at all times and must not be shared with non-staff persons for any reason. When working with Infection Control Practitioners, medical records staff, or other facility representatives on-site, precautions shall be taken so that non-surveillance staff are not allowed to view materials belonging to the HIV/AIDS Surveillance Program that may potentially result in disclosure of confidential information. For example, line lists shall not be held or placed down in such a way that the facility representatives with whom surveillance staff is working can see identifying information about other HIV/AIDS cases.

III. Electronic Security

A. Equipment and Data Storage

The HARS database is now migrated to a web based eHARS system (January 2009). The eHARS server (Server name: HFShi121-03703 (application) and HFShi121-03704 (database)) is located in Commonwealth data center at 101 Cold Harbor. Security at the data center is at highest level. Access is only permitted by getting a secured badge which is kept by COT guards. Connectivity on the eHARS computers in the state network is protected by firewall rules and server access is locked down hard by enforcing group policy. Only two network management personnel have local login access to the server. All computers with the eHARS database must be logged off or turned off at the end of the day, and require a password to login. Access to the eHARS system also requires password authentication. Passwords should not be written down or kept at any place which can be easily accessible. There is a test...
platform for eHARS in CHR server room with two servers namely HFSHI121-03701(application) and HFSHI121-03703 (database). No actual data will be kept on these servers and the only purpose of this platform is to test for updates and may be used for training purposes, with the exception of the eHARS test server. Satellite office staff connects by secure VPN connection to access eHARS system. For backup procedures refer to Section IV. Operational Security, Part C. Record Retention Policies.

A scanning system (SCAN) is used to store electronic copies of the case reports, thereby eliminating the need to retain hard copy case reports long term. Currently the system is running on HFSHI121-0370. This server is located in the COT building in a locked Server Room with authorized access only (i.e., all Office of Technology, OIT, staff). The server is fire-walled off from the rest of the network. Only two network management personnel have local login access to the server. See Section IV. Operational Security and Data Access, Part A. Personnel with Data Access. The application is available remotely only on the three network computers in the HIV/AIDS Surveillance Program central office, and via a secured VPN connection to the network computer in the satellite office. Passwords are required to login to the network computers. An additional password is required to modify any information in the SCAN application. For backup procedures refer to Section IV. Operational Security, Part C. Record Retention Policies.

Both eHARS and SCAN databases are in SQL 2005 database server and each database has its own security rights setup.

The secured shared drive (R:\) also resides on HFSHI121-0370. NTFS permissions on the folder allow access only to authorized HIV/AIDS surveillance program staff. Only four network management personnel have local login access to the server and folder, see Section IV. Operational Security and Data Access, Part A. Personnel with Data Access. Confidential information stored within the secured shared drive is password protected.

The public internet and e-mail applications shall not be open while accessing surveillance information in the SCAN database or the any of the other databases in the secured shared folder (R:\). Regular files on the shared drive without confidential information can be accessed simultaneously with internet and email.

At the central office, confidential information is printed to a networked printer physically residing within the central surveillance office. The printer resides on the print server HFSIN121-0372. Printer permissions restrict access to the central office surveillance staff and the Cabinet for Health and Family Services (CHFS) IT administrators.

The use of laptop computers and other portable electronic devices for working with confidential HIV/AIDS information is absolutely prohibited without prior consultation with the COT Network Staff, Operational Security Staff and Surveillance Coordinator. Laptops and other portable electronic devices are to be used only in the event that no other method can be used due to the exhaustion of attempts. The hard drive shall be sanitized using a program immediately following the given task.

Diskettes, USB Flash Drives and storage media (i.e., removable storage devices) that contain surveillance information with personal identifiers must: include only the minimum amount of information necessary to perform a given task; and be encrypted and stored under lock and key when not in use. No removable storage device shall be removed from the HIV/AIDS surveillance offices without the prior approval of the HIV/AIDS Surveillance Coordinator.
Removable storage devices shall be physically destroyed or sanitized using a software program immediately following the given task, except for devices used for backup. See Section IV. Operational Security and Data Access, Part C. Record Retention Policies for information on retaining backup media.

Analysis datasets extracted from eHARS or any other database must be archived as de-identified in the secured shared drive (R:\). The June and December datasets that are archived must be de-identified within 48 hours (2 days) of the data being frozen. Any datasets used with personal identifiers on a regular basis, e.g. for end of period processing, should be used and PGP shredded within 24 hours after use in order to protect the confidentiality of patient information. Analysis datasets must have personal identifiers removed if taken out of the surveillance office or accessed from an unsecured area. See Section IV. Operational Security and Data Access, Part B. Data Release.

IT authorities must obtain approval from the Surveillance Coordinator before adding users to any HIV/AIDS surveillance program application. IT shall maintain logs documenting authorized users. The Surveillance Coordinator shall review the logs on an annual basis.

B. Data Transfer

At the end of each investigation cycle (traditionally 2 weeks), the Surveillance Nurse Consultant from the satellite site shall SCAN hard copy case reports and enter cases into eHARS. See Section II. Physical Security, Part B. Receipt of Confidential Information. The central office surveillance staff shall enter all its cases for the month into eHARS. The central office can view case reports in SCAN and check data entry into eHARS from the satellite office in real time. An encrypted Access database containing the tracking system for pending and completed case reports for the Louisville office shall also be available in real time at the central office.

C. Electronic Laboratory Reporting-

The HIV/AIDS branch has received funding to increase electronic lab reporting capacity. To allow this new technology to enhance the efficiency and reporting time to the HIV/AIDS branch, policies must be in place to address the possibility of errant lab reports. At the date of publication, one company (LabCorp) is participating in ELR testing, but it is anticipated that more will send lab reports electronically in the future.

Process of receiving electronic lab reports-not in use as of June 2014:

LabCorp sends lab results using HL7 codes directly to the Rhapsody Orion system. Then those results that have an error making it impossible to forward to the NEDSS Based System go immediately into a message error queue. The results are then manually reviewed to see what the error is and then forwarded to the appropriate queue.

Lab results without an unknown error immediately go to a routing table. From there using the codes that identify which test types are included, are sent to one of two queues—security assignment queue or the HIV PAM. One person and an alternate have access to the labs in each of the two queues respectively. The HIV PAM is “hidden” meaning that only the IT personnel, health policy specialist and HIV surveillance personnel know that the folder is present. It is not seen on the directory.

Within the HIV PAM the lab results will be translated into an excel spreadsheet. This will allow lab results to be imported directly into eHARS instead of printed onto paper and then manually entered. HIV surveillance personnel will access lab results from HIV PAM daily.
If a lab is delivered incorrectly:
If the lab result is delivered to the message error queue only, then the IT personnel or health policy specialist assigned to this project will see the message and forward to the HIV PAM. All will have signed the HIV/AIDS security and Confidentiality policy. The lab will then be accessed by HIV surveillance personnel.
If the lab result is delivered to the security assignment queue, the assigned personnel will immediately notify the health policy specialist and HIV/AIDS surveillance coordinator. The health policy specialist will contact LabCorp (or other company) to identify the reason the HIV lab result was not routed directly to the HIV PAM (i.e. new code not identified by the routing table). Once identified, the new code will be added to the routing table. The CHFS IT security officer will be alerted to notify the privacy officer of LabCorp that such a breach has occurred and CHFS has remedied the situation within previously outlined protocols. The CHFS IT security officer and the HIV/AIDS surveillance coordinator will document the breach notifying additional Division of epidemiology staff as deemed appropriate. The assigned personnel to the security assignment queue will transfer the HIV lab result to the HIV PAM.

Prior to implementation of new data transfer and data collection methods, the ORP must grant approval. All methods for data transfer and data collection must incorporate access controls.

IV. Operational Security and Data Access

All policies detailing the security and confidentiality measures of surveillance data shall be documented in writing. The policies shall be provided to all staff and IT personnel with access to surveillance data before they are given access to the surveillance information. An electronic version of the Security and Confidentiality Policy shall be maintained on the secured folder (R:\), which allows access for all surveillance staff in both offices. Hard copies of the Security and Confidentiality Policy shall be maintained at the satellite and central offices.

Each employee (staff, contract, or IT) working with confidential information must read and sign the Employee Non-Disclosure Agreement, the Employee Privacy and Security of Protected Health Information Agreement, and the Employee Confidentiality/Security Agreement for Electronic Usage (Appendix 1) before access to surveillance data is authorized. Each employee must annually sign the Employee Non-Disclosure agreement as proof of continued security and confidentiality training. See Section V. Quality Control. All original forms shall be held in the employee’s personnel file and a copy given to the employee. As an added measure of security, all members of the HIV/AIDS Branch, including services, prevention, and support, shall sign the Employee Privacy and Security of Protected Health Information Agreement, and the Employee Confidentiality/Security Agreement for Electronic Usage.

All staff authorized to access surveillance data shall be responsible for protecting their own workstation and devices associated with confidential surveillance information. Staff should not discuss confidential surveillance information while in the presence of persons who are not authorized to access the data. Keys to the surveillance office and file cabinets shall be kept in the possession of authorized surveillance staff, and shall not be shared or lent to others.

A. Personnel with Data Access

Per KRS 214.645 section (3) (g) access to, and receipt of, HIV/AIDS data is restricted to authorized surveillance staff designated by the CHFS. The list that follows details all
personnel involved with the HIV/AIDS surveillance program and the level of data access allowed:

**Overall Responsible Party (ORP)**
Kraig Humbaugh, M.D.
Access to confidential information only on an emergency basis.

**HIV/AIDS Branch Manager**
Karen Sams
Key access to office and access to confidential information on an emergency basis only. Emergency basis is defined as absence of the Surveillance Coordinator, Technician and Epidemiologist, and public health protection is required.

**HIV/AIDS Epidemiologist**
*Julie Nakayima*

**HIV/AIDS Surveillance Coordinator**
Vacant

**HIV/AIDS Surveillance Technician/Research Analyst**
Julie Kauzlarich

**HIV/AIDS Data entry specialist/administrative assistant**
Vacant
Has access to confidential information. Allowed to receive confidential data from laboratories and providers. Signed agreements in Branch Personnel file.

**HIV/AIDS Surveillance Nurse Consultant**
Susan Delph

**Louisville Metro Health Department Surveillance Nurse Consultant- Immediate Supervisor**
Diane Franconia
Key access to Jefferson County office on an emergency basis. Signed agreements in Louisville Site Personnel file, with copies in State HIV/AIDS Branch Manager’s file.

**Louisville Metro Health Department- Medical Director**
vacant
No access to confidential information. Will receive a monthly activity report detailing the completeness and timeliness of case reporting by the Surveillance Nurse Consultant.
HIV/AIDS SURVEILLANCE SECURITY & CONFIDENTIALITY POLICY

STD Control Program
Kim Horner, Tracy Foster, Sheri White, Sheri Brooks, Danielle Yearby
Receive verification of whether a case was reported to the HIV/AIDS Surveillance Program for the purpose of confidential patient counseling. Signed agreement in HIV/AIDS Surveillance Coordinator’s file.

TB Control Program
Teresa Goins
Receives confirmation from the HIV/AIDS Surveillance Program of whether a case co-infected with TB has also been reported to the HIV/AIDS Surveillance Program. Signed agreement in HIV/AIDS Surveillance Coordinator’s file.

IT Personnel
Wintel Server Team: Carols Felix, Samantha Stamper (Ronnie Boggs, Will Lloyd-supervisors)
Database Administration (DBAs): Craig Silvey (SQL), Ashraf Kazmi (primary assignees)
Namrata Ramakrishna (Database Administration Branch Manager)
Cherokee Hall, Jayarama Marella, Prashanth Chiluka (additional assignees)
Office of Technology and Administrative Services (OATS) Team: Greg Martin (Assistant Director), Terri Grimes, Sravanthi Kotica
Additional COT Staff: Scott Criscillis, Justin Wells (Moveit/ FTP site)

Server team has local login access to the eHARS and SQL servers. Have access to log into the servers for IT support purposes. IT personnel can remotely connect to surveillance staff computers only with explicit permission from personnel assigned to that computer or from the surveillance coordinator. Both parties must be present at their stations for remote troubleshooting. IT personnel are responsible for secure physical environment prior to logging into HIV databases. See section II: physical security; a) security of location. Signed agreements in HIV/AIDS Surveillance Coordinator’s file.

Network engineers/Helpdesk support
Ami Ellis, Gerald Hedrick
Have access to log into surveillance computers for desktop support purposes. Can remotely connect to surveillance staff computers only with explicit permission from personnel assigned to that computer or from the surveillance coordinator. Both parties must be present at their stations for remote troubleshooting. IT personnel responsible for secure physical environment prior to logging into HIV computers. See section II: physical security; a) security of location. Signed agreements in HIV/AIDS Surveillance Coordinator’s file.

Louisville satellite office IT personnel
Star Hammersley, Jimmy Smith

In the event that IT personnel need technical support from outside vendors not part of the cabinet, requiring such parties to remotely view HIV related databases or electronic structures e.g. Image API for SCAN related support, this needs to be cleared with the surveillance coordinator first.
B. Data Release

An integral part of public health surveillance is the dissemination of health data to public health agencies, case providers, and the general public. Surveillance data are needed in order to analyze trends in occurrence and prevalence as well as to effectively plan and evaluate prevention and services programs.

Restrictions on data release, however, must be made to ensure the confidentiality of cases. A strict data release policy is necessary because release of certain types of data, even without names, could be used to identify a case. Those individuals granted access must sign the aforementioned confidentiality agreements, with the understanding that the data is to be used only for those purposes listed in those agreements (Appendix 1).

1. Definition of Terms

Certain terms used in the Kentucky HIV/AIDS Program’s data release policy are listed and defined below.

Aggregate data is that which is combined as a group or a total.

Personal identifying information means name, social security number, date of birth, address, and telephone number.

Surveillance data includes all data collected, including personal identifying information.

No restrictions mean that all data may be released without restrictions.

Population size refers to the population of any geographic region in question. This could refer to the state, county, area development district, or zip code. The most recent population estimate should be used to determine population size.

May be released should not be interpreted to mean, “Required to release.” The release of certain case characteristics, such as gender, risk factor and race, is at the discretion of the Kentucky HIV/AIDS Program.

2. Key Components of Data Release

The data release policy of the Kentucky HIV/AIDS Program is based on three main factors: (1) the recipient of the data, (2) population size of the data region, and (3) time period. In no circumstances should data release compromise surveillance activities or affect the public perception of confidentiality of the surveillance system.

3. Surveillance Data Release Criteria
   a. With Personal Identifying Information
      i. Research Purposes
         HIV/AIDS surveillance data with personal identifiers shall not be released for research purposes outside of the surveillance program.

      ii. State Public Health Agencies
HIV/AIDS SURVEILLANCE SECURITY & CONFIDENTIALITY POLICY

No personal identifying information shall be released to any other offices in the state with the exception of the Kentucky STD Control Program, and the TB Control Program. Information may be released to the designated contact(s) in each program. The designated person(s) shall sign the Employee Non-Disclosure Agreement (Appendix 1) before information is released.

STD Control Program - The information shared with the STD Program is only for the purposes of test result verification for confidential patient counseling. The information is also used for purposes of Partner Counseling and Referral Services.

TB Control Program - HIV/AIDS surveillance staff shall only confirm if a case co-infected with TB has also been reported to the HIV/AIDS Surveillance Program.

Other state public health agencies maintaining other disease data stores may request data access. The ORP shall weigh the benefits and risks of allowing access. The other state agency must demonstrate justifiable public health need for access in order for the ORP to consider allowing access. The other state public health agency must have equivalent levels of security to those in the HIV/AIDS Branch Security Policy. The policies regarding data access by the other state public health agency shall be documented in the HIV/AIDS Branch Security Policy and the Employee Non-Disclosure Agreement (Appendix 1) shall be signed before data access may be granted.

iii. Out-of-State Public Health Agencies

Personal identifying information shall only be released to authorized HIV surveillance staff in other states. There are no restrictions on data release to authorized out-of-state HIV surveillance staff. See Section II. Physical Security, Part B. Receipt of Confidential Information.

iv. Nonpublic health purposes

Access to surveillance information for nonpublic health purposes (i.e., litigation, court order, etc.) shall be granted only to the extent required by law. Requests shall be reviewed by the ORP with legal counsel to determine which specific information, if any, must be released.

b. Without Personal Identifying Information

i. Research Purposes

The researcher must submit a request for the data set to the ORP and Epidemiologist, including the variables needed. The following policy shall guide whether the data may be released:

1. Data may only be released if the smallest population size the researcher will examine is at least 1,000 (e.g., if the data set is meant to examine only Asian AIDS cases in Adair county, the data set shall not be released because the population of Asians in Adair county is less than 1,000). The overriding principle is that no data set shall be released that can indirectly identify any individuals.

2. The researcher must abide by the aggregate data release policies developed by the Surveillance Program.

If the research meets the aforementioned guidelines for data release, the researcher shall be referred to the Chair of the IRB. The Chair shall determine if an IRB
HIV/AIDS SURVEILLANCE SECURITY &
CONFIDENTIALITY POLICY

should be convened. If data release is approved, the researcher shall sign a
Memorandum of Agreement before the data is released. This agreement indicates
that the researcher understands the penalties for unauthorized disclosure, assures
the data will be stored in a secured area, and agrees to destroy any storage devices
containing the data set when the research is completed.

ii. State Public Health Agencies
For information requested for research purposes refer to Security IV. Operational
Security Part B3bi. Data Release, Surveillance Data Release Criteria Without
Personal Identifying Information For Research Purposes.
For information requested for non-research purposes refer to Section IV.
Operational Security, Part B3aii. Data Release, Surveillance Data Release Criteria
With Personal Identifying Information For State Public Health Agencies.

iii. Out-of-State Public Health Agencies
For information requested for research purposes refer to Security IV. Operational
Security Part B3bi. Data Release, Surveillance Data Release Criteria Without
Personal Identifying Information For Research Purposes.
For information requested for non-research purposes refer to Section IV.
Operational Security, Part 3aiii. Surveillance Data Release Criteria With Personal
Identifying Information For Out-of-State Public Health Agencies.

iv. Centers for Disease Control and Prevention (CDC)
Data shall be sent to the CDC electronically, without personal identifying
information. The data shall be transmitted via secure access management (SAMS)
website.

4. Aggregate Data Release Criteria
   a. With Personal Identifying Information
      Aggregate data with personal identifiers shall not be released in any circumstance.
   
   b. Without Personal Identifying Information
      Release of aggregate surveillance data to the general public or other agencies of local,
      state or federal government through published reports, grant applications, grant
      progress reports, correspondence, newsletters, oral presentations, public meetings,
      telephone conversations, or press releases, shall be in a format which prevents breaches
      of confidentiality. This requires safeguards in aggregate data releases that would
      prevent any possible calculations that might reveal the identity of infected persons. As
      such, the following Centers for Disease Control and Prevention (CDC) data re-release
      agreement shall be used primarily and the Kentucky policy used on a secondary level
      for geographical regions below the county level with <50,000 population:
      i) CDC’s data re-release policy is attached as appendix III.
      ii) Kentucky’s aggregate data release criteria includes the following:

      • When the population size for the smallest unit of analysis presented is greater than
        or equal to 1,000 there shall be no restrictions on the cell sizes released.
HIV/AIDS SURVEILLANCE SECURITY & CONFIDENTIALITY POLICY

- When the population size for the smallest unit of analysis presented is less than 1,000, then cell sizes less than or equal to five shall not be released. Instead, the comment shall be inserted “less than or equal to 5.” If only one cell in a row or column is ≤5, then the next smallest cell shall be suppressed in order to release the row/column total. In place of this number, a symbol shall be inserted and annotated to reflect this policy.

- Rates shall not be published if the numerator is less than 10 cases.

- Information at a geographic level lower than the county (including zip codes) shall only be released in accordance with guidelines for aggregate data release above (including cell suppression of cases ≤5 and data aggregation of prevalent or cumulative cases). Additionally, prior approval for release of these data shall be provided by the ORP.

c. Risk Factor data
- Risk factor data may be released at the state level in adherence with overall data release guidelines in section 4 B above.
- The smallest geographic area of analysis shall be the Area Development District (ADD) level. Data at the county level or a smaller geographic region may be released with consent of the ORP.
- At the ADD level, risk factor data may be released with suppression of all cell sizes less than or equal to 5 and the comment shall be inserted “less than or equal to 5.” If only one cell in a row or column is ≤5, then the next smallest cell shall be suppressed in order to release the row/column total and a notation inserted in the cell.
- Risk factor data at the ADD level by demographics may be released in aggregates of prevalent or cumulative cases, rather than incidence. One demographic variable may be released for all ADDs, and 2 by 2 tables may be released only for the top 3 ADDs.

In instances where the policy does not clearly specify whether certain aggregate data may be released, consult with the ORP to determine if release of the information may inadvertently identify an infected person.

5. Special Considerations for Data Release
In those cases whereby release of identifying information is required to protect the public’s health, policy shall be based on Kentucky’s confidentiality laws regarding access to epidemiological data, including HIV/AIDS.

D. Record Retention Policy
Retention of the enhanced HIV AIDS Reporting System (eHARS) Database is regulated by the Cabinet for Health and Family Services Record Retention Schedule (Series 04446 and 04447). These policies require the eHARS database to be maintained permanently within the agency.

Internal record retention policies have been developed to minimize the number of hard copy case reports stored with confidential information. Hard copy case reports will be maintained
HIV/AIDS SURVEILLANCE SECURITY & CONFIDENTIALITY POLICY

for three months after the form is placed in the SCAN system. All reports shall be shredded in a commercial quality shredder within the surveillance office prior to disposal.

All records in the SCAN and eHARS system are permanently maintained. The eHARS system is configured to back up data nightly on the eHARS server. The SCAN database is backed up by the CHFS OIT personnel using IBM Tivoli Storage Manager. Incremental backup, which backs the data up at COT to a storage pool which resides on disk, are performed every night from Monday through Thursday. On Fridays, a full back up on disk is done. Once copied to disk a synchronous copy, which creates another copy onto tape, is created. On Mondays the tapes are sent in a locked container to Kentucky Underground (located in Wilmore, KY - Dept. of Defense approved facility). Weekly full copies are retained for 30 days and monthly full copies are retained for one year. After one year the tapes are recycled for use again, all data is overwritten.

Full database backups are taken every night and transaction log backups are taken every hour. These backups are written directly to a network share on the Data Domain, which is being replicated to the ADC. Full backups are retained for 30 days and transaction backups for 7 days.

Security Violations

For the purposes of this policy, security breaches are defined as those occurrences whereby surveillance staff or others outside the program have allowed the opportunity for a person with HIV/AIDS to be identified, but such identification did not occur. A confidentiality breach is when a person with HIV/AIDS is actually identified by the surveillance program or others outside the program in violation of established policy.

All staff with access to surveillance data shall be responsible for challenging those who are not authorized to access surveillance data. Staff with authorized access to surveillance data shall be responsible for reporting security and confidentiality breaches to the Surveillance Coordinator and the ORP. This includes IT staff and contractors. All staff working in the vicinity of the surveillance offices must question any unauthorized persons in the area and report immediately to the Surveillance Coordinator and the ORP any suspicious behavior. The breaches will be documented in a security log by the Surveillance Coordinator and investigated by the ORP. The investigation shall examine the causes of the breach and determine appropriate remedies.

The ORP shall promptly report breaches of confidentiality to CDC.

The aforementioned signed employee agreements include discussion of possible employment ramifications, as well as criminal and civil liabilities, for any unauthorized disclosure of HIV/AIDS surveillance information and data.

V. Quality Control

Security practices for HIV/AIDS surveillance data shall be reviewed annually by the Surveillance Coordinator. Revisions shall be made, if necessary, and distributed to surveillance staff. Documentation of the annual review shall be indicated by updating the security policy’s revision date.
HIV/AIDS SURVEILLANCE SECURITY & CONFIDENTIALITY POLICY

The addition of new technologies to surveillance activities (i.e., changes in server configurations, software changes, etc.) shall be preceded by an evaluation of existing measures and the development of new measures to ensure the continued security of surveillance information and data. Security practices for the new technology shall be documented in the policy before the new technology is utilized.

For supervisory purposes, the Louisville Metro Health Department Medical Director will receive a monthly activity report detailing the completeness and timeliness of case reporting by the satellite office. The surveillance coordinator will also obtain monthly logs of VPN access from COT to monitor usage of the VPN account.

All staff with access to case-specific information must be knowledgeable about the security and confidentiality policies and procedures. To improve staff knowledge, annual training on the security and confidentiality procedures shall be conducted. The training is required for any staff with access to surveillance data, including servers, backup devices, etc. Each staff shall re-sign the Employee Non-Disclosure Agreement annually to certify their attendance at the annual security and confidentiality training. Reviews of the staff’s compliance with the security policies shall be conducted during the employee’s year-end performance evaluation.

The ORP shall certify, annually, as part of CDC cooperative agreement application that Program requirements are met and security standards are in place.
APPENDIX 1
Employee Non-Disclosure Agreement (Staff or Contract)
Department for Public Health, Division of Epidemiology and Health Planning
HIV/AIDS Branch

The Employee Non-Disclosure Agreement is established in accordance with the following statutes, rules, and regulations:

- KRS 205.175 – Confidential treatment of information and records – Persons to whom furnished
- KRS 214.420 – Records declared confidential – application
- KRS 214.625(5) – Confidentiality of HIV Infection Test Results
- KRS 341.190 – Records and Reports – Confidential treatment
- KRS 434.840-860 - Unlawful access to a computer
- Privacy Act of 1974
- Centers for Disease Control Information Security Standards
- HIV/AIDS Surveillance Program Policies and Procedures

The undersigned employee has been advised that in order to perform the tasks required by the Department for Public Health, Division of Epidemiology and Health Planning, HIV/AIDS Branch, access to confidential information will be necessary. Both the information and the identity of the specific individual to whom the information applies are strictly confidential. Unlawful access to and disclosure of confidential information may result in dismissal and in other penalties including incarceration and fines (KRS 434.840-860), and prosecution may occur as a result of violation of those laws.

In addition, 42 CFR 431.301 – 431.307 states the extent to which medical history record information shall be treated as private and secure. The employee agrees to abide by the following terms and conditions:

1. The employee agrees to use any obtained medical history record information or otherwise classified information only as needed to fulfill the reporting requirements and analytical needs of the Kentucky HIV/AIDS Branch.
2. The employee agrees not to discuss, disclose, or otherwise reveal any medical information or classified information to individuals other than for the purpose of the Kentucky HIV/AIDS Branch.
3. The employee agrees neither to confirm nor deny the existence of any record or classified information on a specific individual to any person not employed by the HIV/AIDS Branch.
4. The employee agrees to immediately notify the Kentucky HIV/AIDS Program Director of any requests by unauthorized individuals for information relating to the Kentucky HIV/AIDS Branch.
5. The employee agrees to abide by the administrative and operational rules and policies developed by the Kentucky HIV/AIDS Branch concerning medical information and classified information.
6. The employee will not map drives that are specific to the HIV/AIDS Branch on a computer to which the said person has access that is located outside of the HIV/AIDS Surveillance office.

I, ________________________________, have read, understand, and agree to abide by the terms and conditions set forth by this agreement.

__________________________________(Signature)
_________________________________ (Date)
If through contract:

____________________________________  ______________________________________
Name of Company                        Company Authorized Representative
APPENDIX II

Cabinet for Health and Family Services

EMPLOYEE PRIVACY AND SECURITY OF PROTECTED HEALTH, CONFIDENTIAL
AND SENSITIVE INFORMATION AGREEMENT

PLEASE PRINT:

<table>
<thead>
<tr>
<th>Last Name, First Name, &amp; MI</th>
<th>Position Number</th>
<th>Department Name</th>
</tr>
</thead>
</table>

I understand that I may be allowed access to confidential information and/or records in order that I may perform my specific job duties. I further understand and agree that I am not to disclose confidential information and/or records without the prior consent of the appropriate authority(ies) in the Cabinet for Health and Family Services.

I understand that all user/passwords to access computer data are issued on an individual basis. I further understand that I am solely responsible for all information obtained, through system access, using my user/passwords. At no time will I allow use of my user/passwords by any other person. I understand my compliance is required, and that intentional or inappropriate use shall result in corrective or disciplinary action up to and including dismissal pursuant to KRS 18A and 101 KAR 1:345. I further understand that installing or adding equipment and/or software without express permission from the Office of Technology is prohibited.

I understand that accessing or releasing confidential information and/or records, or causing confidential information and/or records to be accessed or released, to myself, other individuals, clients, relatives, etc., outside the scope of my assigned job duties would constitute a violation of this agreement and may result in disciplinary action being taken against me, up to and including dismissal. I further understand that employees may subject themselves to civil and criminal liability, as well as disciplinary action, for the disclosure of confidential information to unauthorized persons. I understand all data, information, documents, etc. belong to the Cabinet and I agree not to take any information in any form from the agency upon termination of my employment.

I understand that the following is not an exhaustive list of all confidential information, but is an attempt to include most of the major examples of such information. In the event of doubts about whether certain information is covered by confidentiality requirements, I understand that I should consult my supervisor or the Office of Legal Services.

Under KRS 194A.060, all records and reports of the Cabinet which directly or indirectly identify a patient or client, or former patient or client, of the Cabinet or the Cabinet by a former name (CHR, CHS, CFC) are confidential.

Under KRS 209.140, all information regarding an adult protective service investigation is confidential.

Under KRS 216.530 all inspections of long-term care facilities shall be unannounced.

Revised August 2015
Under HIPAA, an individual’s health care information must be used by the Cabinet and its employees and agents only for legitimate health purposes like treatment and payment. 45 C.F.R. § 160.101, and 160.103 et seq. and specifically §§ 164.500, 164.501, 164.502(a), 164.514 established standards for privacy of health information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Health information that must be kept private and secure is called Protected Health Information (PHI). HIPAA establishes in Federal Law the basic principle that an individual’s medical records belong to that individual and, with certain exceptions, cannot be used, released or disclosed without the explicit permission of that individual or their legal guardian. This includes disclosing PHI in even casual or informal conversation not related to a legitimate health purpose (like treatment or payment) at any time whether at work or not. HIPAA gives consumers of Cabinet programs and services the right to an explanation of their privacy rights, the right to see his/her medical records (with some exceptions), the right to request corrections to these records, the right to control the release of information from their records with some exceptions, and the right to documented explanations of disclosures by the Cabinet and by others who may have access to this information. Those who violate the rules laid down by HIPAA are subject to federal penalties. For non-criminal violations of the privacy standards, including disclosures made in error, there are civil monetary penalties of $100 per violation up to $25,000 per year, per standard. Criminal penalties are imposed for violations of the statute that are done knowingly (on purpose) — up to $50,000 and one year in prison for obtaining or disclosing protected health information; up to $100,000 and up to five years in prison for obtaining or disclosing protected health information under “false pretenses;” and up to $250,000 and up to 10 years in prison for obtaining protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

Under KRS 214.420 and 214.625, all information in the possession of local health departments or the Cabinet concerning persons tested for, having, or suspected of having sexually transmitted diseases, or identified in an epidemiologic investigation for sexually transmitted diseases, is strictly confidential. A general authorization for the release of medical or other information is not sufficient to authorize release of this information. Breach of this confidentiality is considered a violation under KRS 214.990(6).

Under KRS 214.181, no test results relating to human immunodeficiency virus are to be disclosed to unauthorized persons.

Under KRS 222.271 and 42 C.F.R. part 2, treatment records of alcohol and drug abuse patients are confidential and a general authorization for release of this information is ineffective.

Under KRS 216.2927, raw data used by the Kentucky Health Policy Board are confidential. This includes data, data summaries, correspondence, or notes that could be used to identify an individual patient, member of the public, or employee of a health care provider.

Under KRS 202A.091, court records relating to hospitalization of the mentally ill are confidential. Violation of the confidentiality of these records is a Class B misdemeanor under KRS 202A.991.

Revised August 2015
Under KRS 202B.180, court records related to mental retardation admissions are confidential. Violation of the confidentiality of these records is a Class A misdemeanor under KRS 202B.990.

Under KRS 210.235, all records which directly or indirectly identify any patient, former patient, or person whose hospitalization has been sought are confidential.

Under KRS 211.902, the names of individuals are not to be disclosed in connection with lead poisoning records, except as determined necessary by the Cabinet Secretary.

Under KRS 211.670, lists maintained by hospitals, and all information collected and analyzed, relating to the Kentucky birth surveillance registry (concerning birth defects, stillbirths, and high risk conditions) are to be held confidential as to the identity of the patient. Violation of this confidentiality is a Class A misdemeanor under KRS 211.991.

Under KRS 213.131, unauthorized disclosure or inspection of vital records is unlawful. Violation of the confidentiality laws for vital statistics is a Class B misdemeanor under KRS 213.991.

Under KRS 199.570, all adoption files and records are confidential and are not open to any person or entity that does not meet the requirements of KRS 199.572, except upon order of the court which entered the judgment of adoption.

Under KRS 205.175, all public assistance communications, both written and oral, generated during the course of business are confidential and privileged. KRS 205.835 prohibits the unauthorized use of information by an employee.

Under KRS 205.730(6), all child support parental locator information is confidential.

Under KRS 205.735, all child support information supplied by an employer is confidential.

Under KRS 205.796, no employee or agent of the Commonwealth shall divulge confidential child support records unless the disclosure is authorized in a manner prescribed by KRS 205.715 to KRS 208.800.

Under KRS 205.8465(4), no employee of the state Medicaid Fraud Control Unit, the Office of the Attorney General, the Office of the Inspector General, or the Cabinet for Health and Family Services shall notify the alleged offender of the identity of the person who in good faith makes a report required or permitted by KRS 205.8451 to 205.8483, nor shall the employee notify the alleged offender that a report has been made alleging a violation of KRS 205.8451 to 205.8483 until such time as civil or criminal proceedings have been initiated or a formal investigation has been initiated. Any information or report concerning an alleged offender shall be considered confidential in accordance with the Kentucky Open Records Law, KRS 61.870 to 61.884.

Under KRS 434.850, accessing any computer or computerized information without authorization, or causing any such access without authorization, is a Class A misdemeanor.
Under KRS 610.340, all juvenile court records are confidential and shall not be disclosed to unauthorized persons unless ordered by a court for good cause.

Under KRS 620.050, all child protective service investigative records are confidential and shall only be released in accordance with the provisions set forth in KRS 620.050.

Under KRS 625.045, any and all records in a voluntary termination action are confidential and shall only be open to inspection with a written order or as authorized by the provisions of KRS Chapter 199.

Under KRS 625.108, any and all records in an involuntary termination action are confidential and shall only be open to inspection with a written order or as authorized by the provisions of KRS Chapter 199.

Under 7 C.F.R. 272.1 (c), all Food Stamp records are confidential and may only be used or disclosed in accordance with the provision set forth in 7 C.F.R. 272.1 (c).

Confidentiality of family planning services is required by 42 C.F.R. § 59. Section 59.11 states: “All information as to personal facts and circumstances obtained by the project staff about individuals receiving services must be held confidential and may not be disclosed without the individual’s consent, except as may be necessary to provide services to the patient or as required by law, with appropriate safeguards for confidentiality. Otherwise, information may be disclosed only in summary, statistical, or other form which does not identify particular individuals.” The confidentiality rules applicable to all programs or projects supported in whole or in part by federal financial assistance, whether by grant or by contract, are found at 42 C.F.R. § 50.310, which states: “Information in the records or in the possession of programs or projects which is acquired in connection with the requirements of this subpart may not be disclosed in a form which permits the identification of an individual without the individual’s consent, except as may be necessary for the health of the individual or as may be necessary for the Secretary [of Health and Human Services] to monitor the activities of those programs or projects. In any event, any disclosure shall be subject to appropriate safeguards which minimize the likelihood of disclosures of personal information in an identifiable form.”

Under 42 C.F.R. § 431.305, the following types of information relating to Medicaid applicants and recipients are confidential: “(1) Names and addresses; (2) Medical services provided; (3) Social and economic conditions or circumstances; (4) Agency evaluation of personal information; (5) Medical data, including diagnosis and past history of disease or disability; (6) Any information received for verifying income eligibility and amount of medical assistance payments (see Sec. 435.940ff). Income information received from SSA or the Internal Revenue Service must be safeguarded according to the requirements of the agency that furnished the data and; (7) Any information received in connection with the identification of legally liable third party resources under Sec. 433.138 of this chapter.” Under 42 C.F.R. 431.306, all Medicaid records of applicants and recipients may only be released in accordance with the provisions set forth in 42 C.F.R. 431.306.

Under 45 C.F.R. 205.50, all financial assistance programs’ records are confidential and may only be released in accordance with the provisions set forth in 45 C.F.R. 205.50.
Under Internal Revenue Code (6103, 7213, 7213A, 7431) all federal tax information is confidential. Unauthorized disclosure or inspection of federal tax information is unlawful. Violation of the confidentiality laws for federal tax returns is a felony punishable by monetary fine ($5000) and/or imprisonment (up to five years).

I understand that other types of information may also be protected by confidentiality, and that if in doubt as to confidentiality, I should not volunteer information before making certain that the information may be disclosed.

By affixing my signature to this document, I acknowledge that I have been apprised of the relevant laws, regulations, and policies concerning access, use, maintenance, and disclosure of confidential information and/or records which shall be made available to me through my employment in the Cabinet for Health and Family Services. I further agree that it is my responsibility to assure the confidentiality of all information that has been issued to me in confidence even after my employment with the agency has ended. I have read the above, received a copy of the Cabinet’s Confidentiality Policy, and understand my responsibilities.

____________________________  ________________
Employee Signature                Date

____________________________  ________________
Supervisor Signature             Date