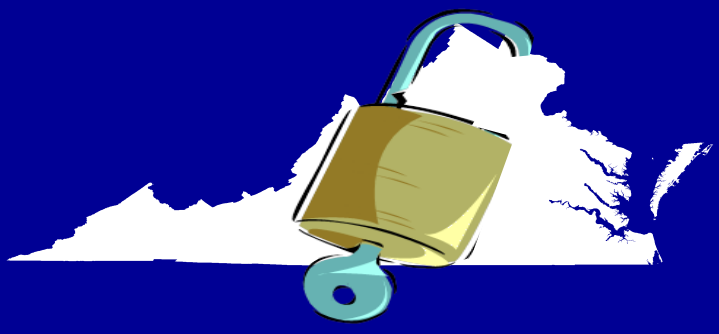
Security and Confidentiality

Policies and Procedures



Division of Disease Prevention
Office of Epidemiology
Virginia Department of Health

This page intentionally left blank

DOCUMENT REVISION HISTORY

Section	Title	Revision Date
	Initial version of Security and Confidentiality Guidelines	CY2000
	New version of the Security and Confidentiality Guidelines	March 2009
4.3	Data Release Procedures (formally titled “Research Access”)	11/24/2009
7.0	Procedural Review for HIV/AIDS/STD/TB Security and Confidentiality, and Timeline	11/24/2009
	New version renamed Security and Confidentiality Policies and Procedures; based on December 2011 CDC guidance.	May 2014
	Updated Table 1: Authorized Access to Confidential Areas/DDP Critical Databases, and Section 7.4 A. Facsimile	5/29/2014

TABLE OF CONTENTS

PREFACE

The Division of Disease Prevention ("the Division") is located in Richmond, Virginia. The Division, along with four other divisions and a business administration unit, provides the framework for the Office of Epidemiology within the Virginia Department of Health.

The mission of the Division is to maximize public health and safety through the elimination, prevention, and control of disease, disability, and death caused by HIV/AIDS, viral hepatitis, other sexually transmitted diseases and tuberculosis. The Division ensures a basic level of health screening of all Virginia refugees.

Historically, this document was referred to as the Security and Confidentiality Guidelines but is now renamed as the Security and Confidentiality Policies and Procedures. Some content from the previous Guidelines document remains, along with additional information and revisions. The Division of Disease Prevention's Security and Confidentiality Policies and Procedures is written to adhere to all standards of the Centers for Disease Control and Prevention National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention *Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs: Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action.*

The surveillance of HIV/AIDS, Viral Hepatitis, STDs, and TB data are principle functions used to shape the Division's prevention and treatment activities. This document includes security and confidentiality policies and procedures for the management of patient level data. It serves as the official policy and procedural guidance for the Division of Disease Prevention pertaining to confidentiality and security of all data under the provision of the Division's programs. These include operational, electronic, and physical safeguards for protecting information.

Certain text within these policies and procedures is more applicable to Division staff, as opposed to external contractors and/or data recipients of potentially identifiable patient level data. By signing the Verification of Receipt and Assurance of Key Requirements and/or the Data Recipient Agreement, Division staff and external contractors/data recipients are agreeing to these policies and procedures. External Contractors and/or data recipients that receive or handle confidential data for or from the Division are ensuring that their respective security standards are at least equivalent to the standards described in this document.

1. INTRODUCTION

1.1 Background

According to the Joint United Nations Programme on HIV/AIDS (UNAIDS): Guidelines on Protecting the Confidentiality and Security of HIV Information[1], three interrelated concepts have an impact on the development and implementation of protections for sensitive data. These are privacy, confidentiality, and security. ***Privacy*** is both a legal and an ethical concept. The legal concept refers to the legal protection that has been accorded to an individual to control both access to and use of personal information and provides the overall framework within which both confidentiality and security are implemented. ***Confidentiality*** relates to the right of individuals to protection of their data during storage, transfer and use, in order to prevent unauthorized disclosure of that information to third parties. ***Security*** is a collection of technical approaches that address issues covering physical, electronic, and procedural aspects of protecting information collected as part of routine data/database management and/or surveillance services.

While the use of health data allows us to protect communities, we must carefully balance it with individual's right to privacy and confidentiality. Overall, the guiding principles of defining health information confidentiality and security should be based on human rights principles. The ultimate goal of public health data security and confidentiality is to minimize patient level disclosure risk while maximizing appropriate availability of data for population health outcome assessment and policy development.

1.2 Purpose

The Division of Disease Prevention's Security and Confidentiality Policies and Procedures (hereafter referred to as the S & C Policies and Procedures) is intended to ensure privacy, confidentiality, and security principles of the Division's patient level information. It is based on guidance from the Centers of Disease Control and Prevention (CDC) National Center for HIV/AIDS, Viral Hepatitis (VH), STD, and TB Prevention (NCHHSTP) *Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs: Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action*, as well as Commonwealth of Virginia laws and regulations.

This document serves as a reference to policies and procedures that ensure the confidentiality and security of information and data collected by and for the Division's programs. The policies and procedures also assist with the Division's compliance with relevant agency, state and federal laws, regulations, and policies concerning the security and confidentiality.

1.3 Usage

The S & C Policies and Procedures contained in this document are to be followed by all ***Division staff*** (hereafter referred to as ***Users***). This includes classified employees, wage employees,

[1] Joint United Nations Programme on HIV/AIDS (UNAIDS): Guidelines on Protecting the Confidentiality and Security of HIV Information, Geneva Switzerland: Interim Guidelines. 15 May 2007. This document is available at: http://data.unaids.org/pub/manual/2007/confidentiality_security_interim_guidelines_15may2007_en.pdf

internal contractors, students, and interns. External contractors/data recipients who perform work for, or in collaboration with the Division must also follow the S&C Policies and Procedures. Any deviation from the procedures or policies within this document must have prior supervisory approval.

1.4 Reporting Regulations

Regulations pertaining to disease reporting within the Commonwealth of Virginia are listed in the State Board of Health's *Regulations for Disease Reporting and Control*.

Relevant sections of the *Code of Virginia* pertaining to the Division include:

Reporting ..... *§ 32.1-36 and 32.1-37*
HIV Testing and Counseling Requirements ..... *§* 32.1-37.2
Confidentiality ..... *§ 32.1-36.1, 32.1-38, 32.1-41 and 32.1-71*
Authority of Commissioner ..... *§ 32.1-40*
Anonymity of Patients/Providers ..... *§ 32.1-41*
Deemed Consent ..... *§ 32.1-45.1*
Isolation of Certain Persons with Communicable Diseases of Public Health Significance ..... *§ 32.1-48.04*
Breach of Medical Information Notification ..... *§ 32.1-127.1:05*
Additional STD Requirements ..... *§ 32.1-56*
Duty to Protect ..... *§ 54.1-2400.1*
Minors' Access to Care ..... *§ 54.1-2969*
Infected Sexual Battery ..... *§ 18.2-67.4:1*
Reportable Disease List ..... *12 VAC 5-90-80*
Those Required to Report ..... *12 VAC 5-90-90*
Prenatal Testing ..... *12 VAC 5-90-130*

1.5 Guiding Principles

The CDC-NCHHSTP has defined 10 guiding principles as a backbone for all *program requirements and security considerations*[2].

1. Public health data should be acquired, used, disclosed, and stored for ***legitimate public health purposes***.
2. Programs should collect only the minimum amount of personally identifiable information necessary to conduct public health activities.
3. Programs should have strong policies to protect the privacy and security of ***personally identifiable information***.
4. Data collection and use policies should reflect respect for the rights of individuals and community groups and minimize undue burden.

---

[2]Centers for Disease Control and Prevention: ***Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs: Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action.*** Atlanta, Georgia: U.S. Department of Health and Human Services, Centers for Disease Control and Prevention; 2011. The document is available at: http://www.cdc.gov/nchhstp/programintegration/docs/PCSIDataSecurityGuidelines.pdf

5. Programs should have policies and procedures to ensure the quality of any data they collect or use.
6. Programs have the obligation to use and disseminate summary data to relevant stakeholders in a timely manner.
7. Programs should share data for legitimate public health purposes and may use data-use agreements to facilitate sharing data in a timely manner.
8. Public health data should be maintained in a secure environment and transmitted through secure methods.
9. Minimize the number of persons and entities granted access to identifiable data.
10. Program officials should be responsible and trustworthy stewards of public health data.

1.6 Resources

Numerous documents from the Virginia Department of Health (VDH), other governmental agencies and private organizations are referenced in this document for ease of accessibility.

A. Virginia Legislative Code

The *Code of Virginia* is the statutory law of Virginia and consists of codified legislation by the Virginia General Assembly. Specific sections within the *Code of Virginia* pertain to the Division and must be followed at all times. These sections provide definitive regulations for all health related issues.

B. VDH

The VDH Madison Building Security Procedures must be followed by all VDH employees working within the Madison Building. The Madison Building Security Procedures were updated in October 2009. The Procedures provide security policies for staff entering the building and for visitors entering the Madison building.

The VDH Confidentiality Policy (OCOM #1.01) was disseminated in May 2011 to provide all relevant policies relating to confidentiality. All VDH employees must become familiar with this policy and follow its provisions in their day-to-day activities. The on-line training for the Confidentiality Policy must be completed annually by all VDH employees.

The VDH Client Safety Event Reporting Policy must be followed any time an unusual event may impact a client or need to be brought to the attention of agency risk management. Staff are responsible for completing the Client Safety Event Reporting form, located within the VDH Reporting Policy, when ***Division management*** deems it necessary.

The VDH Employee Code of Ethics Policy is to be adhered to at all times to promote ethical behavior. It governs behavior in situations that may jeopardize or compromise an employee's moral and ethical standards in the workplace. The Code of Ethics commitments include obeying the law, complying with policies and procedures and maintaining confidentiality.

The VDH Information Security Policy and the VDH Information Security Standard comprise the security framework that VDH uses for Information Technology (IT) systems and information security. Both documents are equally important in discussing a sustainable consistent approach to safeguarding information across all VDH programs.

C. VITA

The Virginia Information Technologies Agency (VITA) has an Information Technology Resource Management (ITRM) Standard by the Commonwealth of Virginia that must be adhered to by all VDH employees. The VITA ITRM Standard document addresses several important topics including: Personal Computer (PC) use, computer access security, ***disaster recovery***, and data security.

D. CDC

The CDC-NCHHSTP *Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs: Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action* was released in December 2011. This new document represented a major revision to the previous guidelines promulgated by CDC and required that the Division's Security and Confidentiality Policies and Procedures be modified to adhere to the standards set forth.

E. NIST

The National Institute of Standards and Technology (NIST) Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) is a Special Publication by the U.S. Department of Commerce. The NIST document provides recommendations for protecting ***confidential information***, as well as ways to respond to an incident or ***breach*** involving ***Personally Identifiable Information (PII)***.

F. Library of Virginia

The Virginia Public Records Management Manual[3] is a document by the Library of Virginia that provides records retention guidance for all public records. In order to have an effective records management program, each agency and locality must implement Library of Virginia-approved Records Retention & Disposition Schedules, document destruction of scheduled records, and disseminate policies and guidelines. The Virginia Public Records Management Manual is a mandate of the *Code of Virginia.*

G. Glossary and Abbreviations

The Glossary of Terms (Attachment 1) defines words contained within this document that may need explanation. The Glossary includes terms that are newly introduced, uncommon, or specialized. The Abbreviations (Attachment 2) identifies a letter or group of letters taken from an abbreviated word or phrase within this document. The Abbreviations are shortened forms of a word or phrase used within this document to represent a complete form.

[3] The Virginia Public Records Management Manual is available at: http://www.lva.virginia.gov/agencies/records/manuals/vprmm.pdf

2. STAFF RESPONSIBILITIES

2.1 Roles and Responsibilities

A. Overall Responsible Party

The Director of the Division serves as the ***Overall Responsible Party (ORP)*** for the security and confidentiality of all data and physical resources. The Director of the Division is the ORP, so throughout this document the term Division Director will be used to refer to this position. The Division Director signs applicable CDC grant documentation pertaining to surveillance and prevention, activities on a yearly basis, and certifies appropriate handling and maintenance of security measures. This includes ongoing review of evolving technology to ensure security and confidentiality of relevant information and establishment of appropriate measures to ensure proper delivery of revised security and/or confidentiality information to the Division's users. The Division Director may make any necessary modifications to policies and procedures in order for standards to be met. The S & C Policies and Procedures should be reviewed at least annually, and revised as needed. The Division's *Security and Confidentiality Program Requirement Checklist* shall be used for such reviews (Attachment 18). If standards cannot be met, reasons should be documented and plans to address these standards should be outlined. Programs must self-certify annually that they are adhering to all of the security standards. In addition, programs should periodically assess whether changes in personnel, programs, organizations, or priorities require changes in policies and procedures.

B. Site Security Officer

The Division Director has designated routine oversight and maintenance of the Division's security and confidentiality activities to the Director of STD Surveillance, Operations and Data Administration (SODA). As such, this position serves as the Division's ***Site Security Officer*** (SSO).Throughout this document the term SODA Director will be used to refer to the SSO. All security-related issues and/or concerns shall be reported immediately to this position. This position maintains oversight and signature authority of security-related accessibility to the Division's physical site locations, as well as database(s) and IT network-related accessibility. The SODA Director also maintains the Division's oversight of staff security training completion.

C. User Responsibilities

All users are individually responsible for state property directly issued to them during the course of employment. Such property may consist of office door keys, file cabinet/desk keys, state identification/building access cards, parking permits, cell phones, pagers, removable or ***external storage devices***, portable devices, computer hardware, software, etc. Each user assumes responsibility for ensuring physical security and proper handling of all devices (see Access Controls, Physical Access). All users who are authorized to access ***Protected Health Information (PHI)*** are responsible for protecting their own workstation, laptop, and/or other devices. This responsibility also includes the protection of User Identifications, also referred to as user names or login names, and passwords/codes that would allow access to PHI (see PC Workstation Accessibility).

Users are responsible for immediately reporting any known or suspected breach or violation of confidentiality or security to their immediate supervisor and/or the SODA Director. Supervisors

should document all incidents via the Incident Response Form (Attachment 5). This includes any suspicious activity or unauthorized use of software or hardware devices/equipment or inappropriate activity associated with PHI. Similarly, the SODA Director should be contacted whenever passwords or other system access control mechanisms are lost, stolen or inadvertently disclosed. This should include all unusual systems behavior such as misrouted messages, missing files, suspicious activity on a PC, or frequent system crashes of unknown cause. When possible, users should try to contain the incident damage and minimize the risk of further destruction. If a computer may be infected with a virus, turn it off immediately. If it appears that the incident might have resulted from inappropriate actions from someone else, the appropriate analysis needs to be performed by IT professionals to determine if evidence can be preserved.

When sending or receiving mail containing confidential information, users should ensure it is sent in a manner that does not allow contents to be revealed. The number of documents per envelope shall be kept to a minimum. All such information should be folded towards the inside of the documentation prior to placement inside an envelope (see Postal/Mailing Services).

Confidential information should not be disclosed over the telephone without first confirming that the recipient is allowed access to the information. When leaving voicemails or sending text messages, users should not state patient identifying information or terms easily associated with surveillance or risk factors (see Telephone). Confidential information should only be faxed when absolutely necessary and users must exercise the utmost caution (see Facsimile). No confidential information should be transmitted via non-secured e-mail, either internally or externally (see Electronic Mail). The confidential information should not be held without confirming that the person is allowed access to the information. The user should not state patient identifying information or terms easily associated with surveillance or risk factors.

It is the responsibility of all VDH employees to be familiar with the VDH Code of Ethics Policy[4], which promotes ethical behavior and aids in the performance of public responsibilities by requiring adherence to agency core values. The Code of Ethics is located within the internal VDH webpage. It includes an important agency commitment for all employees to maintain confidentiality of sensitive patient and client information, employee records and other private information.

If a user discovers any technological issue that appears to elude existing security practices, it should be brought to the attention of the immediate supervisor. Technology and procedures used to secure data is constantly evolving and it is important that the Division maintains an ongoing assessment of security practices. In addition to the above issues, each user is individually responsible for the following: 1) maintaining confidentiality of all Division data and information; 2) ensuring clearance of all issues that may pose a conflict of interest.

[4] VDH Code of Ethics Policy is available at: www.vdh.virginia.gov/pdf/Code%20of%20Ethics.pdf

2.2 Security and Confidentiality Documentation

A. Verification of Receipt and Assurance of Key Requirements

The Division requires signed documentation indicating receipt and understanding of its S & C Policies and Procedures from all persons working for the Division, or on projects involving Division-specific activities and/or data. There are two versions of the Verification of Receipt and Assurance of Key Requirements (Attachment 3), which serves as this documentation. One version is for DDP Personnel and the second version is for Non-DDP Personnel. The Verification of Receipt and Assurance of Key Requirements [for DDP Personnel] must be signed by all full-time, part-time, and wage employees, internal contractors, students, volunteers, and interns. The Verification of Receipt and Assurance of Key Requirements [for Non-DDP Personnel] must be signed by all external contractors, service providers, and data recipients. The Verification of Receipt and Assurance of Key Requirements must be signed upon reading and understanding the Security and Confidentiality Policies and Procedures. The Verification of Receipt and Assurance of Key Requirements summarizes many of the core requirements associated with this document, however it is not inclusive of all requirements. Staff must be aware of, and adhere to all requirements within the S & C Policies and Procedures. Any questions about content should be discussed with immediate supervisor(s) prior to signing the Verification of Receipt and Assurance of Key Requirements. All DDP Personnel must give their signed Verification of Receipt and Assurance of Key Requirements [for DDP Personnel] to the SODA Director. All external contractors, service providers, and data recipients are required to sign the Verification of Receipt and Assurance of Key Requirements [for Non-DDP Personnel] and send to the Division with attention to the appropriate contract monitor. All supervisors/contract monitors are responsible for ensuring that personnel sign the appropriate Verification of Receipt and Assurance of Key Requirements. All contract agreements involving patient level information/data must comply with the S & C Policies and Procedures within this document (see External Contractors/Data Recipients).

By signing the Verification of Receipt and Assurance of Key Requirements, users acknowledge an understanding of the Division's Policies and Procedures and agree to abide by such policies throughout the course of employment with, or through, the Division. In addition, users acknowledge that the regulations governing the confidentiality and disclosure of information related to surveillance data are mandated by the *Code of Virginia* and that the regulations are therefore not necessarily limited to current employees of the Division.

The Division's S & C Policies and Procedures may be accessed on the Division's shared server environment at M:\MISCELLANEOUS\Policies Procedures & Guidelines\security & confidentiality guidelines. It may also be found in the Division of Disease Prevention Operations Manual[5]. Copies of this manual are distributed to Division and pertinent local health department staff.

[5] HIV/STD Operation Manual is available online at: http://vdhweb/std/OperationsManual/index.asp (internal VDH link only)

B. Security Training

All staff with access to Division data and/or resources (including external contractors, and mail room staff) are required to read and fully understand the S & C Policies and Procedures upon hire and annually thereafter. Policies and procedures will be communicated to all Division staff in the annual S & C Policies and Procedures training course to be administered via TRAIN Virginia. Division staff will be required to complete training annually for both the S & C Policies and Procedures and the VDH Confidentiality Policy (OCOM #1.01). However, in person training may be conducted if TRAIN is unavailable, based on supervisory approval. In such instances, the supervisor must provide one of the Division's TRAIN super users with a list of staff who received the in-person training such that employee transcripts are updated. The supervisor will be responsible for ensuring TRAIN is updated for all such staff. All users must also complete the Cyber Security Awareness Training via TRAIN. Documented security training completion for the S & C Policies and Procedures will be maintained as TRAIN transcripts for audit purposes.

3. PLANS, POLICIES & PROCEDURES

3.1 Disaster Recovery Plan

The disaster recovery plan for the Division of Disease Prevention, or Continuity of Operations Plan (COOP), provides the framework for the Division to restore essential functions in the event of an emergency that affects operations. The COOP provides information on how the Division will sustain the capability to perform essential functions during and after disruption in internal operations whether caused by severe weather, other natural and man-made disasters, or malevolent attack. This plan will be used only in the event it is needed. The COOP plan is distributed and/or made accessible electronically to all Division staff, based on specific program area processes. Training is provided to personnel with identified responsibilities. The COOP is reviewed annually and updated, as needed.

3.2 Data Stewardship

A. Guidance

1. Health Insurance Portability and Accountability Act (HIPAA) - ***The Health Insurance Portability and Accountability Act (HIPAA)*** privacy regulations created national standards for the protection of medical record privacy and other personal health information. The United States Department of Health and Human Services (HHS) issued the HIPAA regulations and the Office of Civil Rights maintains responsibility for implementation and enforcement. The HIPAA privacy regulations limit how Protected Health Information (PHI) is shared, prevents employers from using PHI in employment decisions and requires employers to establish safeguards for PHI handling. HIPAA contains both civil and criminal penalties for violations of the regulations. Further information about HIPAA regulations is available at the Office of Civil Rights website.

2. CDC- The CDC-NCHHSTP *Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs: Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action* address the use of both identifiable PII and non-identifiable information. PII is referred to as any

information about an individual that is maintained by an agency. Examples of PII include, but are not limited to:

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as social security number, passport number, driver's license number, taxpayer identification number, or financial account or credit card number
- Address information, such as street address or e-mail address
- Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g. retina scan, voice signature, facial geometry)
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, education information, financial information)

3. Virginia of Freedom Information Act (FOIA)-Patient-level data collected under Section 32.1.-36 of the *Code of Virginia* shall be exempt from the provision of the Virginia Freedom of Information Act (FOIA). This information is considered confidential. "No report published by [a] nonprofit organization, the Commissioner, or other person may present information that reasonably could be expected to reveal the identity of any patient. Publicly available information shall be designed to prevent persons from being able to gain access to combinations of patient characteristic data elements that reasonably could be expected to reveal the identity of any patient." (*Code of Virginia*, Section 32.1-276.9). Release of any statistical information shall also follow common statistical disclosure principles, including numerator and/or denominator rules, and be based on a best practice mentality that seeks to provide reasonable protection of patient identity as expressed via the Code of Virginia. All VDH personnel must be cognizant of the Virginia FOIA as it impacts their work. Data requested under FOIA guidelines will be assessed and determinations will be made regarding FOIA applicability by the SODA Director , Division Director, and the VDH FOIA Coordinator. Employees should refer to the VDH Guidance Document: Responding to FOIA Requests located on the internal website for assistance.

4. VITA ITRM Standard- The Virginia Information Technologies Agency (VITA) has IT-related standards for information systems. These standards must be adhered to by all Commonwealth of Virginia agencies and is the guiding document(s) upon which the VDH Information Security Policy and Standards are based. Policies in the ITRM Standard SEC501-01 are applicable to VDH and may extend, clarify, and strengthen procedures specified in this document.

5. VDH Policies- The Virginia Department of Health has policies and procedures related to confidentiality and information security standards. These policies apply to all VDH personnel including classified employees, wage employees, volunteers, assignees (including students), internal contractors, and employees of local government. The

Division's expectations contained within this document are required to be followed in addition to the VDH Policy.

a. VDH Confidentiality Policy (OCOM #1.01)[6] - The VDH Confidentiality Policy (OCOM #1.01) requires staff to take all necessary precautions to appropriately protect confidential information in their day to day activities. The Confidentiality Policy defines, identifies, and establishes key components regarding management of confidential information by VDH personnel. It pertains to all oral, paper based and electronic confidential information.

b. VDH Information Security Policy[7]- The VDH Office of Information Management and Health IT (OIM) has established an Information Security (IS) program built on the concept of public trust and provides a sustainable approach to information safeguards. The Information Security Policy provides the VDH IS program with a framework of information security best practices for all VDH units to use in securing their information. The function of this policy is to protect VDH IT systems from credible threats, whether internal or external, deliberate or accidental.

c. VDH Information Security Standard[8]- The VDH Information Security Standard establishes specific standards for the VDH IS program and is applicable to all VDH business units. HIPAA requirements, to which VDH must adhere, are included in the IS Security Standard. The purpose of the Standard is to ensure the confidentiality, integrity, and availability of VDH's information assets. IS Standards include security roles and responsibilities; risk management; business impact analyses; IT contingency planning; information systems security; logical access control; data protection; facilities security; personnel security; threat management; IT asset management and data security.

6. Protected Health Information Terminology- There are multiple words referring to confidential health information that are similar in meaning.
CDC uses the term Personally Identifiable Information (PII) within the CDC-NCHHSTP *Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs: Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action.* HHS uses the term Protected Health Information (PHI) throughout the HIPAA regulations. Within the VDH Confidentiality Policy (OCOM #1.01), VDH uses the term Protected Health Information (PHI) and ***Personal Information (PI)*** to refer to confidential information regarding employees,

[6] VDH Confidentiality Policy (OCOM #1.01) Effective: May 19, 2012. Available online at: http://www.vdh.virginia.gov/OEMS/Files_Page/trauma/VDH-OEMSConfidentialityPolicy.pdf
[7] Virginia Department of Health Information Security Policy. Version 1.0. June 2011. http://vdhweb/oim/security/informationsecuritymanual/documents/2012/word/vdh security_policy_version 1.0.doc (internal VDH link only)
[8] Virginia Department of Health Information Security Standard. Version 5.0. August 2011. http://vdhweb/oim/security/informationsecuritymanual/Documents/VDH%20Information%20Security%20Standard%202011/VDH%20IS%20Standard%20V.05%202011/VDH%20Information_Security_Standard%20Version%205.0_%208%2026%2011.doc (internal VDH link only)

clients/patients, and the public as well as other forms of confidential information related to proprietary and/or business information.
In order for agency documents to sync in terminology, VDH's Confidentiality Policy (OCOM #1.01) term PHI will be used primarily throughout this document.

B. The Concept of Least Privilege

The Division maintains all surveillance and other patient-level information securely and confidentially, categorizing all patient records (paper and electronic) within the Division as "confidential". Confidential information shall be accessed only by a user with the authority to access such information, as delegated, and with an expressed need to access such information. Good judgment shall be exercised by the supervisor, employee and the SODA Director regarding such access. Any confidential communication (written, verbal or electronic) shall be shared with other persons on a strict need to know basis. No confidential information shall be released or access provided to individual(s) without appropriate approvals. Confidential information shall be shared with an authorized individual as designated in Sections 32.1-36.1.A, 32.1-38 and 32.1.41 of the *Code of Virginia,* based on an established need to receive such information. Good judgment shall be exercised regarding the sharing of information. All confidential information shall be used in accordance with specified duties and responsibilities and/or data request stipulations (see Authorized Data and Database Usage).

C. Confidential Data Storage

All HIV/AIDS, STD, Viral Hepatitis, TB, and Newcomer Health documents containing patient identifiers shall be secured at the end of each workday in designated storage areas. In special circumstances and with supervisory approval, such information may be locked in a file cabinet or drawer at the end of the business day; however, this information should remain within the confines of secured Division offices of the Madison building; such instances should be minimal. All documents with identifying information that are no longer needed or required for records retention purposes shall be shredded using a commercial-quality cross-cutting shredder by an approved vendor (see Retention/Disposal of Records).

D. Taking PHI into the "field"

Confidential information shall only be removed from the Division's offices with prior supervisory approval and for the expressed purpose of conducting the official business of the Division (see Field Work). All HIV and STD staff that complete field work must follow the Surveillance & Investigation Site Visit Procedures (Attachment 16) prior to leaving the office and upon return. All confidential information carried outside the Division's offices shall be appropriately safeguarded and shall remain the responsibility of the user until such information is delivered or returned to the Division's offices (see Nontraditional Work Settings). Secured briefcases should be used to transport paper copies of PHI. Name tags with limited contact information should be attached in the event of loss or theft.

E. Incident Handling for Confidentiality Breaches

Guidelines for a risk-based approach for protecting confidentiality of PII, including responding to breaches (incident response) for federal agencies, are described in the National Institute of Standards and Technology (NIST) Special Publication 800-122, Guide to Protecting

Confidentiality of Personally Identifiable Information[9]. The NIST document provides recommendations on how to effectively implement procedures to protect PII within organizations, and serves as the foundation for managing incidents.

Users must immediately report any known or potential breaches of security or confidentiality to their immediate supervisor and the SODA Director. The incident should be reported via the Incident Response Form (Attachment 5) by the supervisor and submitted urgently to the Division Director. The supervisor or SODA Director should immediately inform the Division Director of further details regarding the incident. For any known or suspected breaches involving Information Technology (IT), networking data systems, hardware, and/or software, the agency's Information Security Officer (ISO) must also be notified. The SODA Director, supervisor, and any other relevant staff, shall immediately investigate the suspected breach to assess cause(s), implement remedies and, through consultation with applicable VDH staff and/or the Attorney General's office, determine whether the violation warrants reporting to appropriate law enforcement agencies. If a violation is determined to result in the release of confidential and/or private information about one or more individuals (breach of confidentiality), the incident should be reported within one hour to the relevant program manager who will then contact the Information System Security Officer (ISSO) of NCHHSTP and put into place necessary steps. The program manager shall inform the Division Director. It is then determined whether the Incident Response Form (Attachment 5) should be completed, as well as any other documentation required by the Division Director. Copies of all such documentation shall be provided to the SODA Director. When assessing a reported incident, it must be determined whether PHI was released during the incident and if so, how many records or individuals were affected. As directed by the Division Director in consultation with the HIPAA privacy officer, the Division must notify affected individuals and determine whether to provide them with remedial assistance.

Staff may also need to complete the VDH Client Safety Event Reporting Form[10] based on the events assessment done and direction from Division management. When a user must complete the Client Safety Event Reporting Policy, it should be given to their immediate supervisor within the same day.

If PHI is inadvertently disclosed within an e-mail (sent/received) the user should immediately notify their supervisor of the possible e-mail breach. The user should not forward the e-mail containing the personally identifiable information (ex. patient name). If the email was sent by an outside source, notify the sender of the incident but do not reply to the original e-mail.

When PHI is being mailed to the Division, it is important for the mail handler within Central Registry Unit to maintain close communication with supervisors and inform them, when necessary, if packages are delayed. Incident Handling Summary Procedures for Suspected

[9] National Institute of Standards, and Technology (NIST) Special Publication 800-122, available online at: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

[10] The Client Safety Event Reporting Form is available at: http://vdhweb/Procurement/Forms.htm- scroll down and click Client Safety Event Reporting Form (internal VDH link only)

Confidentiality Breaches (Attachment 4) should be followed if delayed, lost, damaged or misdirected mail contains PHI. Refer to the Procedure for Mailing Confidential Patient Information (Attachment 8) for specific details on handling confidential mail.

The incident handling plan should continually be updated and improved based on lessons learned during each incident. Lessons learned might also indicate the need for additional training, security controls, or procedures to protect against future incidents.

F. Access Controls

Users are individually responsible for all state property issued to them during the course of employment and must return upon request and/or at termination of employment (see User Responsibilities).

Computers, external storage devices/peripheral equipment and software shall not be removed from VDH, for any reason, without prior supervisory approval. This excludes staff assigned a notebook PC/docking station or external storage devices such as flash/thumb drives.

All state issued equipment such as copiers, fax machines, telephones, including cell phones, pagers and computers, as well as software and applications, such as email and databases, are for official state use only. Any misuse related to these items will be handled on an individual basis. Supervisory approval must be obtained for any extenuating circumstances regarding the use of state property.

Access to Division resources (e.g. databases, network security groups, folders, patient files) are restricted to authorized users. Each user must be uniquely identified and authenticated. User IDs and passwords will be used and changed regularly, as appropriate. All logon IDs and passwords shall be safeguarded, and passwords shall not be revealed to others. Users are responsible for all activities performed under their assigned logon ID. If a system is misused under an employee's password, the employee is responsible. Always exit any confidential database when not in use. Access to databases shall be password protected (see Computer Security).

Each user of workstations, laptops, cell phones, or any other external storage device assumes all responsibility for ensuring physical security and proper handling of the device. This includes controlling appropriate access to the device, regardless of the environment it is used (e.g. home, office, field, etc.). All staff with a laptop/docking station should ensure that a security cable is appropriately attached to the laptop and locked while in the docking station. In addition, all laptops used by staff that handle PHI must have VITA ***encryption*** software installed on the PC to minimize inappropriate access in the event of loss or theft (see Computer Security and Nontraditional Work Settings). Each user is responsible for ensuring such encryption software is included on their notebook/laptop/tablet.

External storage devices (IronKey™ flash drives) are provided to select users based on a defined need for such equipment. No personal storage devices (smart phone, MP3 player, etc.) are allowed to be connected to or used with state IT equipment. Users with flash/thumb drives should ensure that such devices are only used with state-issued equipment. Additionally, no files containing PHI shall be placed on flash drives and removed from the Division's secured areas, without supervisory

approval. Such instances should be extremely rare, have substantial justification for such use, and include use of the agency approved devices, e.g. IronKey™ flash drives.

The state identification/building access cards are for use by the designated user only. The user shall not allow any unauthorized use of such cards. It is the user's responsibility to immediately notify their respective supervisor in the event their identification card becomes misplaced, lost or stolen. Upon resignation or termination of employment, users shall return their state identification/building access card, as well as any parking permits; to their immediate supervisor (see Physical Security).

3.6 Inventory Tracking

A. Software

All software that is purchased and used by Division staff is maintained by the SODA Director. Hard copy media is kept in a locked cabinet when not in use. A logout form is completed when staff require access to software for reinstallation purposes. The form includes the name/date when software is returned. Staff are responsible for any media in their possession and must lock up such software until it is returned. Staff should return such software immediately upon installation. Electronic license files are stored in the secure server environment with limited access. An inventory spreadsheet is also maintained with staff names and registration numbers. All software purchases should be communicated to the SODA Director to ensure inclusion in the software inventory and the software cabinet or electronic file, as appropriate. No software should be maintained by individual staff.

B. Devices

All devices assigned to users (LCD projectors, flash drives, ***Virtual Private Network (VPN) tok*ens**, keys, phones, etc.) are state property and must be returned upon termination of employment. Equipment such as LCD projectors may be checked out for official work-related activities. Some work units may have equipment assigned to them and maintain an individual check out procedure for their respective staff. The SODA administrative assistant maintains a check out process for all LCD projectors and laptops for use by Division staff with a work related need.

Flash drives (ex. IronKey™), phones, VPN tokens, etc. are assigned and tracked by the appropriate work unit/supervisor. Employees must provide any password assigned to IronKey™ devices to their supervisor upon return of the device. VPN tokens are to be tracked by immediate supervisors to ensure receipt and return.

3.7 Consequences

All workforce members are accountable for their actions related to protection of PHI . Violations of Division of Disease Prevention confidentiality and security protocols, VDH Confidentiality Policy (OCOM #1.01), VDH IS Policy/Standard or ITRM SEC 501-01, will be subject to appropriate disciplinary actions, in conjunction with established Standards of Conduct and/or prosecution under the law as set forth in the *Code of Virginia*, Chapter 2, Title 32.1 and any other applicable regulations.

4. PHYSICAL SECURITY

4.1 Building Access/ Identification Cards

Most VDH staff are housed at the James Madison Building, located at 109 Governor Street Richmond, VA. The building is protected by an electronic security system and security guards that monitor building access and movement. The Office of Purchasing and General Services (OPGS) has specific Virginia Department of Health Madison Building Security Procedures[11] that all VDH employees must follow. According to the Madison Building Security Procedures, all personnel must swipe their state employee identification (ID) card in order to enter the building. The ID card is used to access the building at specific entrances and shall be swiped by all users upon entering the building at all times. It is not permitted to let others "piggy-back" off of your access and enter the building without swiping in or signing in with building security. By using ID cards every day, a listing of employees in the building can be produced in the event of an emergency situation. The ID card includes a color photo and user name, and must be visibly displayed at all times while on state property. If staff forget their ID card, they must show appropriate identification (such as a driver's license) to the security guard and sign into the building.

4.2 Visitors

All DDP visitors must sign in and out with the guard at either the Main Floor (MF) entrance or the lower basement (LB) entrance and provide photo identification. The guard will issue a Visitor's Badge, which must be worn in a visible location while in the Madison Building. When leaving the building, visitors must sign out at the same location where they entered the building and return the Visitor's Badge to the guard.

In addition to the VDH Security Guards, all Division staff are required to maintain awareness and control of visitors (non-Division staff) requesting access to or within the confines of any of the Division's confidential areas. Staff are required to inform the security guard stations (1st floor - Mezzanine and Lower Basement) of any expected visitors with a list that includes: 1) visitor's names; 2) date and location of the meeting; 3) contact name/phone number/office name OR call the guard station(s) to provide the information. If you are unsure as to which door the visitor(s) will use to enter the building, provide the information to both guard stations so visitors can enter at either location. Staff expecting visitors to the 2nd floor shall inform the 2nd floor reception desk (Central Registry Unit) and are responsible for escorting the visitor(s) to designated locations. Division staff shall also walk visitors out of all confidential areas upon completion of meetings, visits, etc.

If unexpected visitors (visitors that have not been previously identified to the guard) arrive, they will not be allowed to enter the building. The respective staff must authorize entry into the building by either 1) appearing at the guard station or then escorting the visitors to their office; OR 2) providing a verbal approval to the guard over the phone.

[11] Virginia Department of Health Madison Building Security Procedures. October 14, 2009. Available online at: http://vdhweb/purchase/Docs2009/Security%20Procedures%20Madison%20Building.doc (internal VDH link only)

4.3 Division of Disease Prevention Offices

The Division is located on the 1st, 2nd and 3rd floors of the James Madison Building All physical locations of HIV/AIDS, STD, TB, and VH information (including workspace for users with access to PHI information) are housed in the 1st, 2nd, and 3rd floors of the Madison Building. The 1st and 2nd floors are considered secured areas that have limited access, based on ID badge access control. Within the 3rd floor, TB information is stored in a locked file room for authorized users only. Access to office locations requiring ID badge access is managed by the Office of Purchasing and General Services (OPGS); authority for granting access to these secured areas is managed by the Division Director, based on work-related justification to such facilities and/or PHI .

4.4 File Room Access

Within the confine of the 2nd floor of the James Madison building, paper copies containing identifying information are housed inside two locked file rooms. One such room is designated solely to HIV/AIDS surveillance data and the other is for STD/HIV testing/VH information. Within the 3rd floor, paper copies containing TB information are housed within a locked file room. Only authorized users may enter record storage rooms and/or receive or review such confidential documents.

Within the confine of the 1st floor of the James Madison building, paper copies containing PHI are housed inside locked, immobile file cabinets, with access maintained by staff who work within this location. Only authorized users have access and/or receive or review such confidential documents.

All confidential information shall be maintained within the above mentioned file rooms and/or cabinets. Staff should retrieve necessary data on a daily basis and return all confidential information at the end of their workday. No PHI should be left in staff offices during non-work hours. Good professional judgment is required when determining if documents require locking during the workday.

VDH janitorial staff access these floors after normal work hours. Therefore, access control for file rooms has been adjusted to require dual ID badge accessibility and a four-digit manual keypad code. Only authorized Division staff have access to these rooms. This dual locking process eliminates cleaning/janitorial staff, who may have universal ID badge access, from being able to access these rooms. All file storage rooms are identified only with generic names to avoid unnecessary observance of where such records are maintained. All rooms are also located within interior office space absent of any windows. Users with access to these areas shall not set the manual locks to remain open, thereby reducing the security level of these areas.

4.5 Records Retention

The records retention rooms in the Upper Basement of the James Madison building, as well as off-site hold records that are no longer needed within the file room but still must be held for retention purposes prior to disposal. The storage room in the Upper Basement is a secure ID badge controlled area, and includes a manual punch code for limited access. The off-site storage room is secured electronically for authorized entry and includes manual key access for staff to enter designated areas. Only authorized staff are allowed to enter into the records retention rooms.

5. COMPUTER SECURITY

5.1 Access

Computer(s) containing electronic surveillance data must be enclosed inside locked rooms/floors. Authorized Division staff have access to the common work areas; however, only appropriate surveillance staff have access to electronic data systems and/or file rooms containing hard copy records. The Division Director may decide that other authorized Division staff need to work inside common areas shared by surveillance staff. All such staff will have signed these same policies and procedures related to security and confidentiality.

5.2 Advanced Encryption Standards (AES)

Portable devices that receive, store, or transport PHI must incorporate the use of encryption software that meets standards detailed in Federal Information Processing Standards (FIPS) Publication 197, ***Advanced Encryption Standards (AES)***. VITA uses Sophos SafeGuard and Guardian Edge software for encrypting Windows 7 and XP operating systems, respectively. All staff with installed encryption software are required to check refreshed/replaced machines to ensure all encryption software and security measures are on their current computer.

A. IronKey™ Flash Drives

IronKey™ flash drives should be used when an electronic storage device is needed to store confidential data. This device encrypts all data with software that meets AES standards and cannot be turned off or accidently disabled. An IronKey™ will erase all data stored after 10 incorrect password attempts. Supervisors should maintain an inventory of IronKey™ devices via the unique serial number at the bottom of each IronKey™. Users should also ensure that they include relevant contact information in the IronKey™ set up process in the event of loss of the device. Any IronKey™ containing confidential data must be maintained separately from a laptop and held securely when not in use. This helps to ensure that loss or theft of a laptop does not include an IronKey™ device. ***Decryption keys*** (i.e. IronKey™ passwords) must be maintained separately. Upon return of the IronKey™ when no longer needed and/or termination of employment, device passwords should be provided to supervisors. All users must exercise necessary precautions not to infect data-related software and hardware with computer viruses and not to expose equipment to extreme temperature variations. External storage devices should only be used for pre-authorized activities.

5.3 Antivirus Software

VITA/NG Partnership staff maintains an inventory of all computers and computer-related equipment. All accessories are logged per VITA/NG Partnership procedures. All software updates to be added to workstations will be performed by the VITA/NG Partnership staff, unless administrative privileges have been granted, based on user defined business need and Partnership agreement. Antivirus software is currently installed on all workstations and servers. This program has been established to automatically update virus definitions on a regular basis and deploy emergency updates, when needed. Users may not disable or modify this software in any way.

5.4 Virtual Private Network (VPN)

The Virtual Private Network (VPN) is an option for staff to remotely access the VDH network. Requests for VPN access must be submitted by the supervisor via the COV Account Request Form.

Approved users may access the COV network via a single factor or dual factor VPN account. Dual factor authentication requires use of a token and is reserved for staff requiring server access. Logging into confidential data systems and/or other files and data sources containing PHI shall be limited to an absolute need for such access while using the VPN. Such access shall only be conducted in the absence of all other persons. Remote access to e-mail, network files and/or data systems shall not be left unattended at any time, regardless of circumstance, while using the VPN.

5.5 Internet Usage

Internet users are expected to represent themselves and the agency with integrity. Each user is responsible for their own activities on the internet and must exercise common sense, professionalism and good judgment. Internet access is closely controlled by security devices, software and configurations designed to provide a highly secured and well monitored environment. Only authorized internet connections via state-issued equipment will be allowed and all connections must conform to the agency's architecture.

Internet usage should be allocated specifically to conducting the Division's business activities. When using the internet, it is not acceptable to violate federal, state or local laws; copyright laws; database license agreements; contracts, policies, or standards; security rules or other expectations. Similarly, it is not acceptable to engage in any activity that is deliberately offensive or creates an intimidating, disruptive or hostile environment for the Division; invades the privacy of individuals; or gains unauthorized access to other computers, resources or entities. Abuse of internet access will be addressed through Standards of Conduct.

Division staff with authority to maintain aspects of the Division website must do so based on established and current procedures. No updates should be performed without the written consent of appropriate Division managers. At no time shall any PHI that could compromise patient confidentiality be uploaded to the Division's web pages. Questions regarding web postings should be directed to the SODA Director for further direction. Division staff with authority to maintain aspects of the Division website must do so based on established and current VDH procedures.

5.6 Network Accessibility

The VDH contracts with the VITA/NG Partnership for all IT network operations. All confidential databases are maintained within the COV network; however, user rights to specific servers, files and databases are controlled by Active Directory. All network users have unique passwords that require forced changes at defined periods. Each user must log on using their credentials and may not log on for the purpose of providing another user access to the network. Standard security configurations, including network access and password management, are maintained by the VITA/NG Partnership and follow the ITRM Standard policies and procedures prepared by the VDH OIM[12].

The Director of SODA serves as the approver for all Division staff network access via Active Directory Security Groups. These Security Groups control access to specific data and files. Security

[12]Password Management in Policies and Procedures. Prepared by the VDH Office of Information Management available online at: http://vdhweb/OIM/policies/Information_Management.asp#53 (internal VDH link only)

Groups are also used to provide access to non-web based data systems. Actual user names and passwords for DDP applications are managed by SODA. Maintenance of network accounts is performed by the VITA/NG Partnership. Staff must follow the Procedures for Establishing and Managing Network Domain and DDP Database Access Accounts (Attachment 13) in order to have COV account access, remote email, and database/data system access.

Intruder lockouts occur once an incorrect password has been attempted several times. Only the system administrator (VITA/NG Partnership staff) can reset a user's network account. All requests for access to the Division's network and e-mail are administered via the online COV Account Request Form (https://esupport.virginia.gov/accountrequest/). Supervisors are required to submit this form on behalf of an employee. The Steps to Completing the COV Account Request Form must be followed in order to complete a request (Attachment 14). All Division submissions are routed to the SODA Director and their designee. The SODA Director approves and forwards requests to the VCCC.

5.7 Database Accessibility

Confidential databases used by the Division are maintained solely by Division staff. Database access is structured with rights limited to staff whose job requires such access. User accounts and rights are set up and maintained by the applicable Data Manager or designated back up. Any changes to user accounts must be approved by the SODA Director. Data Managers should review database account access at least annually and document the findings.

All requests for access to the Division's databases are administered by the Division's Account Request form. Supervisors are responsible for completing the first two sections of the form and forwarding to the SODA Director who approves access privileges and forwards the form to the appropriate Data Manager for user name and password creation. When completed, the Data Manager signs and returns the form to the SODA Administrative Assistant for official filing and audit reporting. The Data Manager will meet with the respective user and provide the new user a login name and password. The Data Manager shall not e-mail such user names and passwords.

5.8 System Administrators

In order to be in compliance with VITA IS Standard SEC 501-01, System Administrators must have both an administrative account and at least one user account. Systems Administrators must use their administrative accounts only when performing tasks that require administrative privileges. At least two individuals must have administrative accounts to each IT system, to provide continuity of operations.

5.9 PC Workstation Accessibility

All users authorized to access PHI are individually responsible for protecting their own workstation, laptop, and/or other devices. This responsibility also includes the protection of User Identifications, also referred to as user names or login names, and passwords/codes that would allow access to PHI. Users may not share their access or disclose their credentials (user ID, password, pin, etc.) or other authentication information with anyone under any circumstances. These requirements make every user solely accountable for all actions from his or her account.

Each workstation is configured with a password-protected screen saver, which will lock the computer after 15 minutes of non-use. This hinders entry by unauthorized users. When users log on, they must acknowledge the legal disclaimer that all activity may be monitored.

Users should log off their workstations at the end of each workday. Users with PCs that access confidential information shall ensure that such databases are closed and the PCs are locked (Ctrl+Alt+Delete) when leaving the work area for periods of time such as lunch breaks. When PCs are left unattended for short durations such as bathroom breaks, PCs should be locked. Any special directions given by OIM referring to PCs must be followed by all users.

Any PC in a non-secure location used to access or utilize confidential information shall only allow such access while the employee is physically located at the PC. Any absence from the PC, such as bathroom breaks, requires that the database be completely closed; turning off the monitor is unacceptable in such locations. The PC monitor must also be situated such that it cannot be easily viewed by persons other than the user. All users are required to report any suspicious activity involving their PC immediately to their supervisor.

5.10 IT-related Surplus, Redistribution and Disposal

It is the responsibility of the VITA/NG Partnership to ensure that all data is erased from PCs prior to surplus. However, Division staff should also make every effort to ensure that confidential data is removed from PCs. This helps to provide an added measure of security of PHI . All state-issued flash drives that are no longer needed should be returned to supervisors. Such devices should not be discarded in trash cans, etc. When disposing of a CD, DVD, or older floppy diskettes, staff should use special shredders available on the 2nd (Rm. 229) and 3rd floors (mail station).

All PCs that are received by Northrop Grumman for surplus and/or reuse must have their hard drives wiped. DBAN/Tech Disposal software is used to wipe hard drives. Based on the ITRM Standard document, before the removal processes begins, the computer should be disconnected from any production network to prevent accidental damage to the network operating system or other files on the network. There are three acceptable methods to be used for hard drive data removal methods: overwriting, degaussing, and physical destruction. If the hard drive is inoperable and has reached its useful life, it shall be physically destroyed or degaussed. Clearing data (deleting files) is not an acceptable method of removing Commonwealth data from agency or storage provider hard disk storage media. Hard drives shall be destroyed when they are defective or cannot be repaired for reuse. PHI data, which should be stored on a COV device, requires at least a three-pass overwrite with at least one pass being random. Following this, the software should provide verification based on a pass check for random patterns. Any use of this software must be approved by the Chief Information Officer (CIO) and the Information Security Officer (ISO) prior to use, and the Office of Information Management must maintain documentation for audit purposes.

The VITA/NG Partnership has established procedures for removal of files/information on IT equipment. The VITA/NG Partnership maintains responsibility of all hard drive sanitation and/or removal of all data prior to any redistribution. If a PC is redistributed to another user within the Division, VITA/NG staff should perform a check of the PC and with the applicable users to ensure confidential data is absent from the machine. Methods used to sanitize a storage device must ensure that any data on the device cannot be retrieved by using “undelete” or other data retrieval

software. Hard drives, flash drives, or any other storage media of computers that once contained identifying information must be sanitized or physically destroyed before the equipment is labeled as excess or surplus, reassigned to other staff members, or sent-off site for repair.

6. DATA SECURITY

6.1 Physical Access

Surveillance information or other PHI shall only be removed from secured areas of the Division for the expressed purpose of conducting official business of the Division. Supervisory approval must be provided in advance and documentation of the occurrence must exist, including specifics regarding the data (Attachment 16). Variables that could link a specific person to a reported communicable disease must be removed from surveillance information prior to removing from the secured area of the Division. Hard copy surveillance information removed from the Division offices must be maintained in locked brief cases at all times. When securing electronic data, the preferred method is with whole device encryption. HIV/AIDS surveillance data must be encrypted, using AES encryption standards, before the SODA Director approves it for electronic transfer to CDC. VH, STD and TB related data transfers should follow similar procedures as a best practice, whenever feasible. Additional databases or other electronic PHI files used by surveillance staff should also be encrypted when not in use, or at the very least, maintained in a secure network environment accessible only to staff with a defined need for such access.

All removable or external storage devices containing PHI must (1) include only the minimum amount of information necessary to accomplish assigned tasks, (2) be encrypted or stored under lock and key when not in use, and (3) have data deleted immediately after use**.**

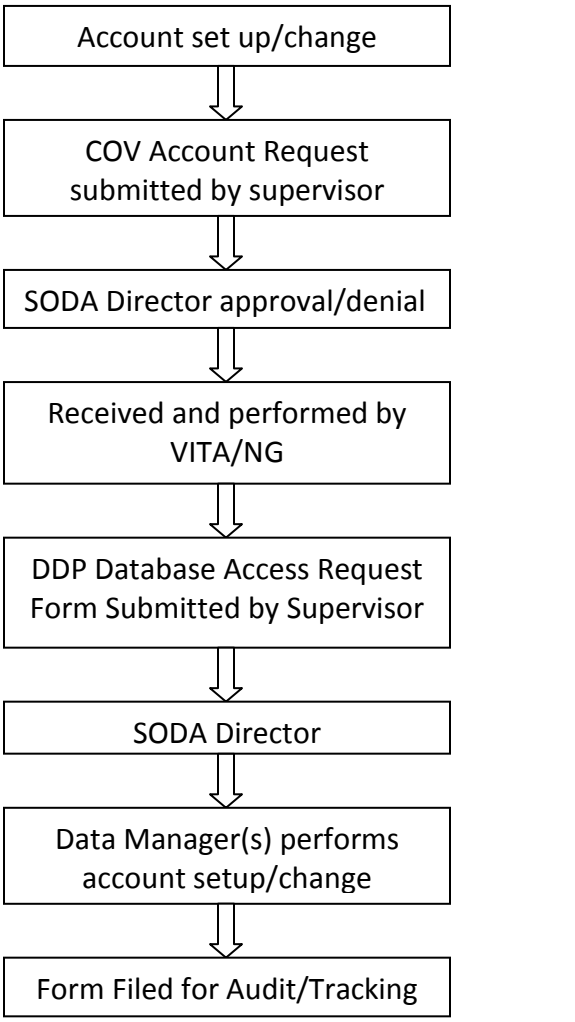
All PHI-related paperwork and removable storage devices must be stored appropriately when users are away from their work areas. This includes proper filing at the end of a workday and appropriate precautions for short durations during work hours. Surveillance information with personal identifiers should not be taken to private residences without appropriate supervisory approval and through documentation. Upon termination of employment, database access should be deleted/disabled. Transmission of any case-specific information that does not incorporate the use of an encryption package (for example by e-mail, fax, phone, or mail) must not use terms easily associated with surveillance or risk factors (for example, HIV/AIDS, VH, STD, TB or any specific behavioral information). Such terms must not appear in the context of the communication, including addresses. Use of such transmissions shall be limited and used only when absolutely necessary. Any electronic transfer of data collection should be approved by the Division Director and incorporate the use of access controls. Whenever identifying information is used, it must contain only the minimum amount of information necessary for completing a given task and, where possible, must be coded to disguise any information that could easily be associated with a given disease or condition.

6.2 Authorized Data and Database Usage

Network access is performed by the Division's VITA/NG Partnership (see Network Accessibility), which provides access to folders and/or security groups where databases are physically located. This process provides a "separation of duties" that assists in limiting unnecessary access to PHI. The

SODA Director provides network folder/security group access approval. Analysis data sets are stored on a segmented local area network (LAN). Staff must go through an approval procedure in order to have network access to specific data analysis folders. User accounts for confidential databases are maintained by the Division's designated Data Managers, with oversight provided by the SODA Director. The SODA Data Administration Manager provides back up support. All security group and database access is controlled by a least privileges concept. This process also ensures that analysis data sets have appropriate storage areas. The data variables within data sets should be kept to the minimum that is necessary. The Network Access Approval Process (Figure 1) depicts the procedure necessary for staff to gain access to HIV/VH/STD/TB information or other personally identifiable data.

Figure 1: Network Access Approval Process



Electronic data files and/or legacy data systems stored for future use (ex. ancillary databases, working laboratory or frozen datasets) should be put into the specific network folders assigned. These specific network folders have restricted staff access within the Division. Microsoft Access databases and datasets should never be copied to a separate location, other than the folder specifically established for these purposes. Only designated staff are assigned to create weekly and/or monthly analysis data sets. A listing of appropriate folders for each type of data is available from the SODA Director.

Identifying information from the Division's databases may be shared/matched with other VDH disease registries in accordance with ***data sharing*** procedures (see Data Sharing). Computer files including personal identifiers shall only be stored on the Division network in designated folder locations. No personally identifiable data files should be stored on PC hard drives (e.g. desktop, C: drive). Authorized access to confidential areas/critical databases (Table 1) is only approved for specific staff based on the need for PHI. Division of Disease Prevention database access shall be deleted/disabled/edited immediately upon termination of employment or a change in duties and responsibilities, using the Division's Database Access Form.

Table 1: Authorized Access to Confidential Areas/ DDP Critical Databases

	Madison Bldg. Storage	Offsite Storage	HIV File Room	STD File Room	TB File Room	eHARS	STD* MIS	ADAP	VACRS	Sentinel STD Surv.	Newcomer Health	CTR	HEP TLC	HIV Data Extract	ELR	NEDSS
Director, Division of Disease Prevention	★	★	•★	•★	•★	★	★	•★	•★	★	★	★	★			★ (HEP) (TB)
Director of SODA	•	•	•	•		★	•	★	★	•	★	★	★			★ (HEP) (TB)
SODA Program Staff (as needed)	•	•		•			•								•	
HIV/AIDS Surveillance Program Staff		★	•	•		•	•							•	•	
SODA Data Administration Manager	•	•	•	•		•	•	★	★	•	★	•	★	•	•	★ (HEP) (TB)
STD*MIS Database Manager	•	•	•	•		•	•			★					•	
eHARS Database Manager	•	•	•	•		•	•	★	★	★		★			•	
HIV Counseling, Testing and Referral Database Manager	•	•		•		•	•					•	★			
Hotline Staff (as needed)		★		★												• (HEP)
Informaticists	•			•		•	•	★	★	•		•			•	• (HEP) (TB)
Epidemiologists (per job duties)	★	★	•	•		•	•	•	•	•	•	•	★		•	• (HEP) (TB)
Data Entry Staff (per job duties)	•		•	•		•	•	•	•	•	•	•	•			• (HEP)
DDP DIS (as needed)	★			•			•									
TB Staff (as needed)	•	•		•	•											• (TB)
Hepatitis C Program Staff	•			•									•			• (HEP)
HCS Data Manager	•	•						•	•					•		
HIV Prevention Program Staff	•	•		•		★	★		★			★				

eHARS: enhanced HIV/AIDS Reporting System

ADAP: AIDS Drug Assistance Program

HEP: Hepatitis

TB: Tuberculosis

CTR: Counseling, Testing, and Referral

STD*MIS: Sexually Transmitted Diseases Management Information System

VACRS: Virginia Centralized Reporting System

NEDSS: National Electronic Disease Surveillance System **[Non-DDP System]**

HEP TLC: Hepatitis Testing and Linkage to Care

• user has routine access

★user has permission for access but may not maintain such access routinely

6.3 Data Release Procedures

A. Research Related Activities

Data that is used for public health research should follow stipulations in Common Rule, Title 45, Part 46, of the Code of Federal Regulations, which includes obtaining both Institutional Review Board (IRB) approval for any proposed research and informed consent of individuals directly contacted for further participation. The proposed research must be determined to serve a legitimate public health purpose. The use of identifiable data for research purposes must be based on a demonstrated need for the data, IRB approval, data confidentiality, conform to Virginia statute §32.1-36.1 and data use sign off, including agreement of final disposition of the data. All such requests must be submitted following procedures outlined on the Division's Data Request Form (Attachment 6). The Division will assess such data requests, based on public health relevance, business need and associated data confidentiality assurances. Access to aggregated non-identifiable health data for research purposes may also require IRB approval, depending on the data requested.

Prior to granting access to the data, the requestor must sign the Data Recipient Agreement (Attachment 7), which certifies that he or she will comply with the Division's security and confidentiality standards. Signing this statement indicates that the requestor (1) understands the penalties for unauthorized disclosure, (2) assures that the data will be stored in a secured area, (3) agrees to return or dispose of any data by an approved method when the research project is completed, and (4) agrees to provide written notice of data destruction. A minimum of five business days, from the date received, should be allotted for Division review and consideration. All ***data releases*** will exclude personally identifiable information, unless otherwise approved by the Division Director. As covered within the data release agreement, such data are solely for the explicit use specified. No additional data extrapolations or usage is permitted, unless additional requests for use are submitted and approved.

B. Data Suppression

The Division will ensure data release procedures incorporate numerator and denominator rules, as appropriate, in a consistent manner that provides for reasonable public health data access. A Rule of 5 (0<X<5) numerator rule will be applied, as necessary, depending on specifics of a data request. A denominator rule (50 per population)[13] will be evaluated for all data of a geographic granularity at or below the city/county level. Prior to any data being released by the Division it must be reviewed and approved for necessary data constraints by the Lead Epidemiologist, SODA Director or Division Director. Epidemiologists working on data sets should always remove identifiable data fields before creating the data set. Routine data quality management and data quality assurance analyses are performed to ensure accuracy of data before being disseminated. In addition, the above numerator and/or denominator rules may be further restricted to ensure added confidentiality, as appropriate.

[13] O'Carrol, P, et al. Public health Informatics and Information Systems. Springer Science+Business Media. Inc. 2003. p204.

6.4 Court Ordered Data Access

All requests for access to confidential data resulting from litigation, court order, subpoena's etc., served to any staff within the Division shall be referred to the Division Director for consultation with the Attorney General's Office, State Epidemiologist and/or the Office of the Commissioner. When information is ordered released as part of a judicial proceeding, any release or discussion of information should occur in closed judicial proceedings, if possible. Staff should never release the name or identifying information of any patient or provider to the media unless approved by the Commissioner.

6.5 Data Collection and Use

The purpose for which data is to be collected should clearly be stated when the data is to be shared or used. When new data collection is being considered, such information should specifically inform the goals of the project. The minimum amount of information necessary to conduct specified program activities should be collected and shared. Collecting data simply because it may be used at a later date or because it is easily accessible should be avoided. Evaluation of data should be conducted to ensure accuracy and validity prior to using data in any capacity. If proposed data collection includes identifiable data, ensure that such data is absolutely necessary. Whenever possible use non-identifiable data for public health purposes and distribute it in a timely manner.

6.6 Data Receipt and Handling

All hard copy data is received in secured areas with limited access. Fax information is sent only in secure areas. Electronic data is received from OIM and stored within secure folders or databases on the Division's servers with limited access.

All reports containing data are secured within file rooms, which are within a secured floor, have electronic card readers, as well as manual code locks. All PHI is returned at the end of each business day to coded file boxes in the file room. Once the boxes become full they are moved to the Upper Basement for continued storage, then the off-site storage unit based on the records retention process.

6.7 Data Sharing

A. DURSA

A DDP Data Use and Reciprocal Support Agreement (DURSA) is forthcoming and will be included in a future revision of the Security and Confidentiality Policies and Procedures. The DURSA will be a formal, multi-party agreement that is entered into voluntarily by all participants. The DURSA will address data sharing among all health-related programs. The DDP Data Recipient Agreement (Attachment 7) currently serves as the Division's data sharing documentation.

B. DDP Programs

Any data sharing must be for a legitimate public health purpose and in accordance with applicable laws and regulations. Any entity with which information is shared needs to have adequate data security and confidentiality protections in place that are consistent with the standards in this document. Non-identifiable data should be shared whenever possible. The amount of information shared should only be the minimum amount necessary.

C. Non-DDP Programs or Entities

Personnel outside the Division's work units may gain access to confidential information only if the request for such information 1) has been authorized by the Division Director; 2) is deemed an expressed and justifiable public health need and/or purpose; 3) does not compromise or impede surveillance or other programmatic activities; and 4) does not negatively affect public perception of confidentiality of data collection activities.

The Division Director will limit such activities to other programs or entities that demonstrate justifiable need for the data or provide enhanced information for public health action. The decision to allow such activity will also be weighed against the benefits and risks of allowing access to specific data and, as necessary, upon certification that the level of data recipient security is at least equivalent to the standards described in this document.

Patient Navigators for disease-specific linkage and retention to care are an example of individuals who may gain access to confidential information. The Coordination of Care and Services Agreement (CCSA) form (Attachment 17) will be used to provide consent from a patient in order to coordinate their medical care and provide needed support services. The form can be used to refer a patient directly to a medical provider or to a Patient Navigator, if those resources are available in the patient's service area. DDP staff must verify the CCSA form has been completed prior to provision of laboratory results.

Data including personal identifiers shall only be transferred or shared with other VDH Offices or Divisions upon approval by the Division Director. However, applicable information, record searches, etc. for local health department personnel may be released. Confirmation of the requestor and/or location shall be performed prior to the release. Any uncertainties regarding the release of information to local health department staff shall be reviewed with supervisors. Any other VDH Office or Division which receives confidential data from the Division shall sign applicable Division policies regarding data release and confidentiality. A ***data sharing agreement*** shall be in effect prior to any routine cross-program data sharing, record searching and/or data matching.

6.8 Data Transport

A. Automated Data Transfers

The agency has established a mechanism for data transmission receipt from healthcare providers or other entities. Rhapsody Integration Engine serves as the primary source of all such incoming data. The ELR Message Receipt and Initial Processing Procedures (Attachment 15) depicts what happens when receiving data involving OIM and Rhapsody.

B. Manual Transfer of PHI

IronKey™ flash drives should be the only external storage device used to transport any electronic PHI and should be done only with justifiable need as well as facility (as appropriate) and DDP supervisory approval. Any paper copies of PHI that must be manually transported should be in a secured briefcase and if necessary to leave in vehicle because that is the safer environment, then necessary steps should be taken to ensure it is out of direct sight by the casual observer. All such records should remain in the personal possession of DDP staff until the documents are secured properly within DDP offices. Such records are not to be transported to home locations without documented supervisory approval.

6.9 Medical Records

Medical records may be viewed at clinic locations via paper, microfilm or electronic form. Staff must follow any guidance set forth by the facility when viewing medical records within a clinic. Medical records should be viewed within a private area of the clinic with limited access.

6.10 Replication of Patient-Level Data

There should be no printing or copying of patient-level data on network printers or copiers outside of secured areas. It is preferable that printing/copying of such documentation occurs within secured offices. All printing/copying shall be removed from printers/copiers immediately. Copies of such data shall be destroyed in accordance with Records Retention/Disposal Procedures. Only the mandatory number of copies of such information shall be copied/printed. Any extra or inadvertent copies shall be shredded immediately. Instances requiring use of copiers in non-secure areas may arise; these circumstances should be conducted with supervisory approval, kept to an absolute minimum and the copier/printer shall not be left unattended.

Photography and video within the confines of any of the Division's secured areas should not be conducted, unless it is necessary for business purposes. This includes the use of any device that produces film or digital photographs, including cell phones with picture and video storage capability. Capture of printed or electronic information relative to PHI could inadvertently be included in such photos or video. If photos are to be taken for work-related purposes, care must be exercised to ensure no PHI is included in the photos.

6.11 Retention/Disposal of Records

All surveillance records are stored within dually secured File Rooms accessible only by authorized users. Records including, but not limited to, surveillance are retained for defined time periods in accordance with Library of Virginia guidelines. Only authorized users have key codes and manual key access to the storage locations for review, retrieval and destruction of such records. Records with personal identifiers needed for historical purposes shall be stored within locked areas.

An on-site storage location for hard copy files is located within the James Madison Building. Access is limited to authorized users only; however, three members of the Office of Purchasing and General Service's (OPGS) management (Director, Deputy Director and Business Manager) are able to gain entry to the room for emergency and safety purposes. Authorized users are required to scan their keycard and enter a security code to gain entry to the storage room. A manual key, which grants an override to the manual lock, is provided to OPGS for the above stated purposes. OPGS is responsible for maintaining the key in a secure location. Members of OPGS shall request access, as necessary, to the storage room through the Division of Disease Prevention, either via the SODA Director or Division Director. Access to the storage room without prior approval or without accompaniment of Division staff should be avoided, unless emergency conditions warrant such access. In such instances, OPGS shall provide written notification of such access, including date, time, personnel involved and reason for entrance. Management of OPGS who have access to the storage room will be required to sign the S & C Policies and Procedures, a copy of which will be maintained by the SODA Director, indicating their adherence to the standards.

Records not stored on site are moved to an undisclosed secure off site location. Authorized users of this location are data management staff, surveillance and Hotline staff. They are required to enter a

security code, in order to gain access to the building. Storage areas are controlled by a separate manual key(s). Access to this offsite location is maintained by the SODA Director. Individual staff must provide a rationale for needing access to this location and promptly return the manual key(s) back to the SODA Director.

STD, HIV, TB, and Hepatitis morbidity records, interview records, field records and/or laboratory records are retained for surveillance-related and historical purposes based on records retention guidance set forth by the Library of Virginia – Records Management Division (General Schedule No. 120). Laboratory slips and consent forms maintained by external contractors, i.e. AIDS Service Organizations (ASOs), Community Based Organizations (CBOs), etc. shall be shredded prior to disposal based on established Library of Virginia schedules. Records meeting the requirement for destruction shall be shredded using a commercial-quality cross-cutting shredder and may be conducted by an approved vendor. Records must be cross cut shredded into pieces ≤ 3/8". Appropriate Division staff must be present at all times during DDP document destruction. Records of destruction shall be provided to Division contract monitor staff immediately after destruction and during site visits. If a contract agency ceases operations prior to document destruction, all lab slips, consent forms and other testing information containing patient names must be immediately returned to the Division for storage and retention. For further information on DDP records retention, see the Records Retention and Disposal Guidelines & Procedures.

6.12 Back-ups of Surveillance Databases

The eHARS (enhanced HIV/AIDS Reporting System) and STD*MIS (Sexually Transmitted Disease Management Information System) surveillance databases are backed up on a daily basis via the VITA/NG Partnership automatically through the existing Commonwealth of Virginia domain. TB and VH surveillance data are backed up according to Virginia's National Electronic Disease Surveillance System (NEDSS) schedule, as those reportable conditions are maintained within the NEDSS system. On Fridays, all data on the Division's servers are backed up. This back up includes all databases plus other relevant Division information.

6.13 Data Transfers

A. Data transferred to CDC

Data transferred to CDC must be encrypted using AES when any moderately or highly sensitive files, any moderately or highly critical information, or any limited access/proprietary information is being transmitted to or from CDC electronically. Such data should be sent via the Secure Data Network (SDN). Per CDC guidelines, the Division uses PGP encryption software for HIV Incidence transfers. STD data transfers do not currently use encryption processes, other than the SDN for weekly morbidity transmissions. TB and VH data transfers are performed via routine NEDSS data transmissions. HIV data is encrypted monthly using eHARS encryption standards prior to data transfers.

All transferred data encompasses only the fields officially requested through CDC data requirements and/or through mutually agreed upon Memoranda of Agreements. All data transfers are performed by the respective Database Manager or designee.

B. External Contractors/ Data Recipients

All Division data managed by external contractors are subject to all policies and procedures within this document. All external contractors shall sign the Verification of Receipt and Assurance of Key Requirements [for Non-DDP Personnel] regarding data confidentiality on an annual basis (see Verification of Receipt and Assurance of Key Requirements). The original copy should be sent to the Division with attention to the appropriate contract monitor. Data transfers to or from external contractors or data recipients are only performed via e-mail if personal identifiers are nonexistent. Any data including PHI approved for analysis by an external contractor or data recipient must be delivered securely without identifiable headers of disease names. Hard copy data transfers including personal identifiers should not include identifiable disease information and should be hand-delivered to applicable personnel inside envelopes without specific indication of the nature of the data. Electronic data transfers must adhere to existing VDH data exchange processes.

Any dissemination of information resulting from data managed by external contractors or data recipients shall be reviewed and approved by appropriate Division staff prior to release. Sufficient time should be allotted for this review procedure. A copy of all final products shall be provided to the Division at the time of dissemination.

C. Maps

The Division provides maps upon request to local health departments and external stakeholders and/or community partners throughout the state to enhance epidemiological capacity and aid in disease surveillance, prevention, and control. Any maps provided for a geographic level that are more specific than county level must be maintained using strict security and confidentiality controls. The level of data sensitivity is dependent upon specificity of the data presented on the map (i.e. point-level data or counts by census tract).

1. **Geocoded Maps for Local Health Departments-** Geocoded maps with street level information of cases/clients or providers shall not be disseminated to data requestors, unless the requestor is from a local health department. Maps with geocoded data must be maintained with strict confidentiality considerations. Although names and addresses are absent from hard copy maps, geocoded data points within a defined area may be sufficient for patient identification. In the event of such requests by local health departments, the map(s) shall be sent to the appropriate Health Director with a memo stating who requested the data. A statement regarding the need to ensure confidentiality of the map(s) should be included in the memo. The requestor should be copied on the memo. The current template used by the Division is as follows:

- ***[Health District Director],***
- *The Division of Disease Prevention has been requested, via* ***[employee name that requested the map(s)],*** *to provide geocoded data and/or disease-specific maps of your health district, or a part thereof, for prevention, and/or educational outreach purposes. The Division sends all such map requests through the applicable District Director to ensure appropriate management of confidentiality and security issues.*
- *Depending on the request, maps may contain street level data of a geographic area (i.e. cities, counties, zip codes, census tracts, etc.). Specific disease data plotted on a street level map presents a different avenue of confidentiality concern, given the geocoded proximity to the patient's address. Maps with this type of detail are virtually the same as a morbidity line list without patient names but with a potentially identifiable address. Plus, geocoded line lists provide for easily identifiable addresses. As such, we ask that you provide appropriate guidance to the health department recipients of such information. As a guide, the Division recommends that maps be displayed in areas accessible only by staff whose access to such data will assist in disease prevention and control. Posting of maps in areas accessible to the public or health department offices unrelated to the project should occur only if the map contains nonspecific data, i.e. ranges of disease occurrence within defined geographic areas. Line lists of geocoded data should only be shared with appropriate staff. The Division also recommends that street level maps and/or geocoded data be destroyed or stored in confidential areas upon completion of associated projects. Health department staff should use caution if uncertain about the confidentiality level of data present on a map.*
- *The requested information will be addressed and mailed to you today, or is attached to this message, depending on the nature of the data. The Division of Disease Prevention hopes you find this information useful and informative as a public health tool for targeted disease surveillance and health education/promotion activities. As always, your feedback is appreciated. Any comments or questions you have regarding the use of geographic information systems for enhancing disease surveillance may be addressed to* ***First Name, Last Name*** *at* ***first.lastname@vdh.virginia.gov*** *or* ***804-864-XXXX.***

2. **Maps for External Stakeholders and Community Partners-** Geocoded maps at the census tract level may be provided to external stakeholders when a map at the county level is not sufficient for disease prevention and control activities. Maps provided are not for use in public presentations or otherwise disseminated beyond program staff directly involved in the intervention and/or grant-related submissions/reports. Since a census tract represents such a small geographic area, it is essential to maintain proper security and confidentiality of the map. In the event of such a request, the program director or most senior leader in the organization should be contacted stating who requested the maps and assurance should be provided that stipulations regarding confidentiality will be followed. Maps provided should be labeled "For Internal Use Only." Confirmation from the program director must be received prior to sending the maps. The current template used by the Division is as follows:

- ***[Employee name that requested the map(s)],***
- *Per your request, the Division of Disease Prevention will provide disease specific maps of your geographic area of interest for prevention and grant purposes. The maps are not intended to be used in presentations or disseminated outside of necessary program staff and/or grant-related submissions or reporting. The Division sends all such map requests through the applicable Program Director to ensure appropriate management of confidentiality and security issues.*
- *This request contains census tract level morbidity counts. As such, we ask that you provide appropriate guidance to the program staff receiving such information. As a guide, the Division recommends that maps be displayed in areas accessible only by staff whose access to such data will assist in disease prevention and control. Posting or storing of maps in areas accessible to the public or other offices unrelated to the project should be avoided.*
- *The requested information will be provided after receiving acknowledgment from the Program Director, [**First Name, Last Name**], that the Division's confidentiality guidance will be followed. The Division of Disease Prevention hopes you find this information useful and an informative public health tool for targeting health education/promotion activities. As always, your feedback is appreciated. Any comments or questions you have regarding the use of geographic information systems for disease prevention may be addressed to **First Name, Last Name** at **first.lastname@vdh.virginia.gov** or **804-864-XXXX**.*

7. DATA COMMUNICATIONS

All phone systems and other communication resources are intended for official state use and authorized purposes.

Any confidential communication (written, verbal or electronic) shall be shared with other users on a strict need to know basis. Confidential information shall be shared with an authorized individual as designated in Sections 32.1-36.1.A, 32.1-38 and 32.1.41 of the *Code of Virginia* only when an expressed need to receive such information is confirmed. Such communication, viewing, or discussions, should be shared only in secured areas. If a secure area is not available, staff should ensure they are using good professional judgment regarding communications (cubicles with high walls, rooms that lock, etc.). Employees shall exercise good judgment at all times regarding the sharing of information.

Transmission of any case-specific information that does not incorporate the use of secured mechanisms (i.e. encryption packages, approved electronic exchange, Tyvek mailing envelopes, etc.) must not use terms easily associated with disease condition or risk factors (for example, HIV, AIDS, Hepatitis, STD, TB or any specific behavioral information). Such terms must not appear in the context of the communication, including sender and recipient addresses and labels.

Whenever identifying information is used, it must contain only the minimum amount of information necessary for completing a given task and, where possible, must be coded to disguise any information that could easily be associated with the specific disease(s).

7.1 VDH Internal Mail Distribution

Internal distribution of documents containing PHI between Division and Office of Epidemiology staff shall be handled in a confidential manner, similar to Postal/Mailing Services. Staff must use

inter office envelopes and avoid leaving envelopes containing PHI in staff mailboxes/inboxes. Whenever possible, information containing PHI should be hand delivered to staff. If staff are out of the office then the information needs to be held until the person is available or provided to the next level supervisor/designee. Ensure the name of the intended recipient is written on the envelope and verbally inform the next level supervisor/designee of the contents.

7.2 Postal/Mailing Services

A. Incoming

Confidential information should be mailed to the Division in a manner that does not allow information to be revealed without opening the envelope. The number of documents per envelope shall be kept to a minimum (≤20 preferably). All such information shall be folded towards the inside of the documentation prior to placement inside envelopes.

Mail containing confidential data should be addressed to appropriate DDP staff. Any envelopes or packages known or suspected to include confidential data-related information should be forwarded to appropriate mail recipients within secured areas on the 1st or 2nd floor to be opened and date-stamped. This practice helps to ensure that confidential information remains unopened while in non-secure areas. If mail recipients are unknown, staff should provide such envelopes to their respective supervisor. All non-confidential incoming mail is date stamped and distributed to appropriate Division staff by administrative staff on the 3rd floor. If confidential information is accidentally opened on the 3rd floor, staff must physically deliver such mail to the appropriate 1st or 2nd floor staff. Specific procedures for mailing documents to DDP are found in the Procedure for Mailing Confidential Patient Information (Attachment 8).

B. Outgoing

Outgoing mail shall follow the same principles of practice as stated above for Incoming mail. Other methods that provide delivery tracking can also be used whenever feasible. The term Division of Disease Prevention should not appear on the envelope if confidential information is enclosed. The return address should be "Virginia Department of Health, Room XXX, 109 Governor Street, Richmond, VA 23219." The terms HIV, AIDS, STD, TB, VH or any specific disease/behavioral information must not appear anywhere in the context of the communication, including the sender and/or recipient address and label.

C. Electronic Media Mailing

Mailing information for programmatic operations may require the use of media (e.g. CD, DVD, IronKey™) to be sent or received. This is not a preferred method for data transfer and should only be used when absolutely necessary. Staff must complete the Electronic Media Mailing Form (Attachment 12) to request approval for mailing such devices. The process needs to be documented and approved by Division management and relevant information security staff prior to mailing any such devices.

7.3 Telephone

A. Incoming

Staff must exercise common sense and good judgment in the use of all voice communication tools. Staff must choose an appropriate voicemail passcode, without common logic associated with the

individual that could easily be ascertained by others. This password should be treated with the same confidentiality as a PC login name and password.

Confidential information is shared over the phone with authorized staff for the purpose of morbidity reporting or for record searching treatment or morbidity history. Assistance with sharing confidential information through incoming calls shall only be completed if staff are confident of the identity of the caller and he/she is an authorized recipient of such information. Uncertainty regarding the identity of a caller should be verified via a call back procedure and/or discussion with appropriate personnel. If a call back verification is performed, staff shall not acknowledge this procedure to the caller. The caller's name, location and telephone number should be obtained and the caller informed that the Division will return their call as quickly as possible. Any uncertainty regarding the caller's location or authorization to receive such information should be immediately forwarded to the appropriate supervisor or the SODA Director. Staff shall not release any information if unsure of the legitimacy or authorization of the caller. In general, all such calls should be forwarded to staff that perform this type of task routinely.

B. Outgoing

Confidential information is shared with persons outside the Division on a strict need to know basis and performed only in secure areas. In general, such calls are performed as a result of follow up to an inquiry or for updates to current morbidity reports and surveillance activities. When outgoing calls are made from the office, "Virginia Department of Health" should be the only information to show up for receivers if Caller ID is being used. Sharing confidential information through outgoing calls shall only be completed if staff are confident in the identity of the recipient of the call and he/she is an authorized recipient of such information. Staff shall not release any information if unsure of the legitimacy or authorization of the recipient. Messages with identifying patient information or terms easily associated with surveillance or risk factors (for example, HIV, AIDS, STD, TB, VH or any specific behavioral information) shall not be left on voicemail systems or via text messaging. Unless otherwise instructed by supervision, these types of calls should only be completed by staff that routinely performs this type of task. Disclosure of confidential information by telephone must also be from a secure or private area whenever feasible. The use of cellular phones or public telephones to communicate confidential information should be avoided.

7.4 Electronic

A. Facsimile

Confidential information should be hand delivered or mailed whenever feasible. Faxing of confidential information is allowable in situations when information is needed immediately, or when mail or courier delivery will not meet a necessary timeframe. Confidential information shall be faxed with caution, using the utmost discretion. Faxed, confidential information must only be sent to, or received at, secure/confidential locations. The Division recipient of such a call should 1) verify the appropriate fax number being used by the caller, and 2) await the facsimile completion and immediately remove such documentation from the fax machine. If incoming faxes are not received within an expected time frame, the staff awaiting the facsimile should contact the sender. Completed facsimiles with confidential information shall not be left on fax machines unattended.

Outgoing facsimile transactions from the Division shall follow the same guidelines as above. Similarly, when confidential information are to be faxed to a new fax number/facility, a test cover sheet should first be sent to a previously identified person and acknowledgement received from the same fax number. After that, sensitive information may be sent. Staff should always double check the recipient's fax number before pressing the send key in order to eliminate misdirected faxes. If the facsimile transmission fails to reach the recipient, check the internal logging system of the facsimile machine to obtain the number to which the transmission was sent. If the sender becomes aware that a fax was misdirected, contact the unintended receiver immediately via another fax and ask that the material be returned or destroyed. Investigate misdirected faxes as a risk management occurrence or security incident, inform the Division Director and complete the DDP Incident Response Form (Attachment 5).

Linking disease status or risk factors with identifiable information about a person must be avoided. This includes using disease coding to reduce the likelihood of comprehension in the event the facsimile is received by unauthorized personnel. Terms associated with surveillance or risk factors of HIV/AIDS/VH/STD/TB must not appear in the fine print at the top of a fax indicating the sender. There is a separate fax cover sheet for each DDP program fax number. Program names are not identified on the fax cover sheet in order to minimize use of PHI. When sending a fax, ensure you are using the fax cover sheet with the correct fax number you want the recipient to send faxes to in the future. The generic fax cover sheet (Attachment 9) must be used as a template for all DDP program fax cover sheets. All fax cover sheets include a confidentiality disclaimer statement and instructions if the document is received in error.

B. Electronic Mail (E-mail)

Confidential information shall not be transmitted via non-secured e-mail (including Outlook), either internally (between Division and/or other VDH staff) or externally (between Division staff and outside sources). Employees and providers shall not e-mail patient names/list, other patient identifiers or geocoded maps. E-mail is not secure and may be seen by more people than the intended recipient. Use of highly secured email systems are used by some state agencies or outside entities. In such instances, VDH staff may be authenticated to such systems and allowed to access/retrieve PHI. Routine data requests without personal identifiers may be sent using e-mail; however, discretion should be used, and assistance from staff routinely performing such tasks should be sought, as needed. When sending an e-mail requesting or inquiring about PHI, users should include text such as the following: "Please do not reply to this e-mail with any patient identifying information. This includes: name, phone number, date of birth, address and medical record number. Please call my confidential line at (804)-864-XXXX to coordinate this exchange. Thank you."

7.5 Internet Partners

When an **internet partner** is elicited during an interview, staff should obtain the complete e-mail address and/or website-specific user ID(s). Only designated and trained staff should send messages to such partners. Confidentiality will be maintained so the partner will only be told that "I need to speak to you about an urgent health matter" and instructions will be given to contact the designated staff.

8. NONTRADITIONAL WORK SETTINGS

Nontraditional work settings may consist of telework locations, as well as field work and other temporary remote sites. It is imperative that staff remain vigilant of security and confidentiality requirements when in such settings. Nontraditional work settings should not have hard-copy storage of client-identified data. If hard copies of documents must be stored temporarily, prior supervisory approval must be obtained (see Physical Access). Double locked file cabinets that are large and heavy enough to render them immobile should be used, if necessary.

8.1 Teleworking

Teleworking is becoming increasingly more common. Staff must ensure that home access is performed using the Commonwealth's VPN (see Electronic Security). The work environment of a teleworker shall be subject to audit to assure that minimum physical security can be verified. A telework location should have work space with limited access in a private area. The ability to observe any PHI (Protected Health Information) must be restricted to only the teleworker. The work space must be configured to allow for confidential conversations, as needed.

8.2 Field Work

DDP staff must present health department identification when performing surveillance/field/follow up activities outside of the office environment. If PHI is required, staff should make every effort to include such data on their IronKey and keep it in a separate place from their laptop. When staff return to the office, PHI should be moved from the IronKey onto a secure network folder and then deleted from the IronKey. No PHI should be stored on a PC hard drive (eg: desktop, C: drive). All discussions pertaining to confidential information shall be conducted in secure, private areas. Medical record reviews shall be conducted as discreetly as possible. Confidential information is never to be left unattended. Staff members shall follow existing procedures related to PHI outside of the office setting (see Physical Access and Taking PHI into the "Field") and ensure that the purpose of their field activity is not apparent to the casual observer.

Line-lists are sometimes carried into the field to assist with active or sentinel surveillance activities. These line-lists shall be de-identified to ensure that the disease and risk status are coded for security and confidentiality purposes. Whenever possible, all notes written by staff should use disease codes to disguise information. Only patient information required for the specific field-related work for that day shall be transported into the field (Attachment 16). No unauthorized pictures or copying of confidential information shall occur in nontraditional work settings. In rare instances when it is absolutely necessary to make copies in a non-secure area, the copier/printer should never be left unattended. Confidential hard copy information should be carried in secure devices at all times. Contact information should be included on all laptop bags, briefcases, etc., in the event of loss or theft. This information should include the staff's name, contact phone number, and email address. Avoid including job title, if it includes disease specific information such as TB Nurse or HIV Epidemiologist. All confidential information carried outside of the offices of the Division shall be appropriately safeguarded and is the responsibility of the employees until such information is returned to Division offices. Hard copies of confidential information should never be viewable from outside of a vehicle at anytime (see Manual Transfer of PHI).If the work does not require an overnight stay, the information should be returned to the Division's secured work area

daily. Prior supervisory approval must be obtained when out of town travel or some other reason precludes returning confidential information the same day. Supervisors must document all events involving staff possession of confidential information in the field and/or taking information to private residences.

8.3 Remote Work (Short Term/Temporary Setting)

In the case of an emergency or outbreak response activities, staff may be detailed to work sites that have not been prepared to meet ideal security standards. It is important that staff ensure the work site is made as secure as reasonably possible in terms of physical, electronic and procedural security. Remote work spaces should still have limited access. Confidential phone conversations should be in an enclosed room or confined area. Use of privacy screens for laptops should be used as an added measure of data security.

All users may access their e-mail via the VITA/NG secure web mail URL. All applicable e-mail, VDH and/or Commonwealth of Virginia policies apply to remote access and use. Users shall also use extreme caution when accessing files, databases and/or printing documents remotely, be mindful of other persons and refrain from any e-mailing of confidential PHI (see Electronic Security). No downloading, except to an approved network location, or printing of files from data systems shall occur at a non-health department location. Printing from a remote location to a health department printer may be allowed when absolutely necessary. All rules used at office locations shall exist for non-health department, remote locations.

8.4 Electronic Security

All PCs/laptops that are used in nontraditional work settings that may access confidential data must have encryption software installed (ex: Sophos SafeGuard or Guardian Edge for laptops or IronKey™ flash drives). In addition, the CISCO Systems VPN Client must be used for staff to access the COV network from a remote location (see Virtual Private Network and Attachment 13). This includes single factor authentication for users accessing COV servers and associated applications. Staff that require access to back end data and functionality for data systems must have dual factor authentication, which requires a ***fob***. Before taking any device containing sensitive data out of a secured area, the data file(s) must be encrypted. COV electronic devices (including flash drives, cell phones, laptops, etc.) shall not be taken outside of the Continental U.S. unless it is based on an approved business need and prior approval from the ISO or CIO has been given for business related travel.

Encrypted flash drives, such as IronKey™, are provided through the Division and should be the only type of flash drive used to temporarily store or transfer confidential data. Decryption keys must not be on the device(s). No personal computers or personal electronic media storage may be used. The device must be issued by the agency and supervisors should maintain serial numbers distributed to each staff. Laptops and flash drives used in the field should be protected from extreme heat and cold. Staff are personally responsible for protecting their agency issued equipment when working in a nontraditional work setting. If the computer is connected to the Internet via Wi-Fi, access to the Wi-Fi connection must be secure. The use of Wi-Fi access in public spaces should not be used if any work related to PHI is involved. Staff should not connect state issued flash drive devices to non-

issued COV PCs. Permission must be obtained if part of a given work activity requires the use of PCs.

Any state issued flash drive that is used for such activity must follow the Procedures for running virus scan on IronKey™ flash drives (Attachment 10). All steps should be followed to ensure virus scans are performed appropriately. Any DDP program that completes a non-COV program activity requiring the use of an IronKey™ or an IronKey™ data transfer process must complete the IronKey™ Flash Drive Operation Activities Form (Attachment 11) and submit to the SODA Director, who will work with the VDH ISO to receive approval for the specified use.

Internet service provider (ISP) or personal network equipment (routers) may be used for Internet connectivity of an agency provided device within a remote location. Users must ensure a secure account connection is used at the remote location. Files or datasets with PHI should never be copied to PCs or other external devices in use at remote locations.

When working in a nontraditional work setting and accessing data systems, access to and use of data files should only occur within appropriate viewed Division file network locations.

9. PROCEDURAL REVIEW OF HIV/AIDS/VH/STD/TB SECURITY AND CONFIDENTIALITY

The Division Director is responsible for all DDP security and confidentiality issues. The Director of SODA is the Division Director's designee responsible for monitoring and ensuring the day-to-day security of the Division's data and associated systems, with assistance from specified staff. Security precautions regarding network administration, access and computer equipment is maintained by the VITA/NG Partnership. Any problems, concerns or recommended changes for the enhancement of Division security should be discussed with the Division Director promptly.

The Security Review Timeline (Table 2) includes Division security activities describing specific items, dates and/or times the items are reviewed or completed, and the Division staff responsible for ensuring completion.

All Division staff will undergo annual training updates/reviews via TRAIN beginning in 2014. After initial training, all staff will be required to re-take the TRAIN course annually. The Verification of Receipt and Assurance of Key Requirements must be signed by all DDP staff and provided to the SODA Director for audit purposes annually. A record of TRAIN course completion will be available for supervisors.

Table 2: Division of Disease Prevention Security Review Timeline

SECURITY ITEM	REVIEW TIMELINE	RESPONSIBILITY
HIV/STD/TB file rooms	Opening/closing report requested and monitored annually, or as needed	Director of SODA
Requests for access changes for e-mail, keys, phones, VPN, databases etc.	Immediately upon an employee's initial employment, termination or change in assigned duties/responsibilities	Immediate Supervisor
Security and Confidentiality Policies and Procedures	1) Annual Completion of S & C training via TRAIN Virginia and Verification of Receipt and Assurance of Key Requirements completion 2) Annual review of TRAIN and Verification of Receipt and Assurance of Key Requirements completion	1) Immediate Supervisor 2) Director of SODA with TRAIN Superusers.
Data Sharing Agreements	Beginning and end of agreement, as needed	Relevant Program Director or Coordinator
Equipment Tracking Processes	Review to ensure equipment return for each instance	Immediate Supervisor
Log of staff field-related activities, including paperwork removal/return to office location	Prior to, and upon return, of relevant staff field activities	Immediate Supervisor
Secure offices	Random checks to ensure doors and file cabinets are locked and confidential paperwork is appropriately filed, etc.	Director of SODA

ATTACHMENT 1:

Glossary of Terms

Advanced Encryption Standard (AES): This standard specifies the algorithm that can be used to protect electronic data and is issued by the National Institute of Standards and Technology (NIST). Publication 197 of the Federal Information Processing Standards (FIPS) contains the specifications of the AES, which can encrypt (encipher) and decrypt (decipher) information. Encryption converts the data back into its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in block of 128 bits.

Breach: A departure from established policies and procedures, or a compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or loss of control of Protected Health Information (PHI) or a departure from established policies or procedures. A breach is an infraction or violation of a policy, standard, obligation, or law. A breach in data security would include any unauthorized use of data, even data without names. A breach may be malicious in nature or purely unintentional.

Confidential Information: Any identifiable information, including, but not limited to, medical and demographic information, that:

1. Reveals the identity of the data subject or is readily identified with the data subject, such as name, address, telephone number, social security number, health identification number, or date of birth; or

2. Provides a reasonable basis to believe that the information could be used, either alone or in combination with other information, to identify a data subject.

Confidentiality: The protection of personal information collected by public health organizations. The right to such protection is based on the principle that personal information should not be released without the consent of the person involved except as necessary to protect public health.

Data release: Dissemination of data either in a public-use file or as a result of an ad hoc request which results in the data steward no longer controlling the use of the data. Data may be released in a variety of formats including, but not limited to, tables, microdata (person records), or online query systems.

Data sharing: Granting certain individuals or organizations access to data that contain personally identifiable information with the understanding of personally identifiable or potentially identifiable data cannot be re-released further unless a special data sharing agreement governs the use and re-release of the data and is agreed upon by the receiving program and the data provider(s).

Data sharing agreement: Mechanism by which data requestor and data provider can define the terms of data access that can be granted to requestors.

Decryption Keys: Unique passwords that allows you to decrypt a file.

Disaster Recovery: Use of off-site computer operations (where copies of data and information systems are stored) to recover data lost as the result of a catastrophe at the primary site of data storage or to activate information systems to replace those lost.

Division management: Refers to the Division Director and appropriate work unit managers and/or designee.

Division staff: All persons working in, or serving for, the Division of Disease Prevention including classified employees, wage employees, internal contractors, students and interns.

Encryption: The manipulation or encoding information so that parties intended to view the information can do so. There are many ways to encrypt information, and the most commonly available systems involve public key and symmetric key cryptography. In general, for both public and symmetric systems, the larger the key, the more robust the protection.

External storage devices: Include but are not limited to CD-ROMs, USB port flash drives (IronKey™), zip disks, tapes, smart cards and removable hard drives.

Fob: A small hardware device with built-in authentication mechanisms. The device displays a number sequence which allows the user to log onto the network. The number sequence on the device constantly changes after a period of time to ensure security.

Health Insurance Portability and Accountability Act (HIPAA): Enacted to ensure continued health insurance coverage to individuals who change jobs and to establish standards regarding the sharing of health information. The HIPAA Privacy Rule protects the privacy of individually identifiable health information. The HIPAA Security Rule sets national standards for the security of electronic protected health information. The confidentiality provisions of the Patient Safety Rule protect identifiable information being used to analyze patient safety events and improve patient safety. However, "the HIPAA Privacy rule recognizes the need for public health authorities responsible for ensuring public health and safety to have access to protected health information to carry out their public health mission. Accordingly, the Rule permits covered entities to disclose protected health information without authorization for specified public health purposes." The HIPAA regulations exclude information considered "education records" under FERPA from HIPAA privacy requirements.

Internet Partner: A person identified as being at risk of an STD based on existing interview data.

Legitimate public health purpose: A population-based activity or individual effort primarily aimed at the prevention of the injury, disease, or premature mortality. Or the promotion of health in a community, including: 1) assessing the health needs and the status of the community through public health surveillance and epidemiological research, 2) developing public health policy, and 3) responding to public health needs and emergencies. Public health purposes can include analysis and evaluation of conditions of public health importance and evaluation of public health programs.

Overall Responsible Party (ORP): The Division Director, which accepts overall responsibility for implementing and enforcing security standards. This position has the authority to make decisions about program operations that may affect programs accessing or using the data, and should serve as contacts for public health professionals regarding security and confidentiality

policies and practices. The ORP is responsible for protecting data as they are collected, stored, analyzed, and released and must certify annually that all program security requirements have been met.

Patient Navigators: Provide assistance with linking and retaining patients in care, assisting patients with additional referrals to support services and necessary resources. Disease Intervention Specialists (DIS) serve in this role as needed, in the absence of a Patient Navigation Program existing in the patient's service area.

Personal Information (PI): All information that: describes, locates or indexes anything about an individual including his or her real or personal property holdings derived from tax returns, and his or her education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment records, or that affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of his or her presence, registration, or membership in an organization or activity, or admission to an institution. PI includes information such as race, sex, age, home address, home telephone number, marital status, dependent's names, insurance coverage, or Social Security Number.

Personally Identifiable Information (PII): As defined by National Institute of Standards and Technology Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), "Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial and employment information."

Protected Health Information/Personal Health Information (PHI): Individually identifiable health information including demographic data, (i) that relates to the individual's past, present, or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and (ii) that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

Privacy: The legal protection that has been accorded to an individual to control both access to and use of personal information that provides the overall framework within which both confidential and security are implemented.

Security: A collection of technical approaches that address issues covering physical, electronic, and procedural aspects of protecting information collected as part of routine data/database management and/or surveillance services.

Site Security Officer (SSO): The SODA Director is designated in this position and is responsible for routine oversight and maintenance of the Division's security and confidentiality activities. This position maintains signature authority of security related accessibility to the Division's physical site locations, as well as database(s) and IT network-related accessibility. The SSO also maintains the Division's oversight of staff security training completion.

Surveillance information: Includes, but is not limited to, case reports, databases, line lists, laptops, removable media, or any other records with identifying information in written, electronic or other format.

Token: see Fob definition

Unit Manager: A DDP employee who oversees one or more program areas and reports directly to the DDP Director.

Users: see Division staff definition

Virtual Private Network (VPN): A network of computers that uses encryption to scramble all data sent through the Internet-making the network virtually “private”.

ATTACHMENT 2:

Abbreviations

AES	Advanced Encryption Standards
AIDS	Acquired Immune Deficiency Syndrome
CDC	Centers for Disease Control and Prevention
CIO	Chief Information Officer
COOP	Continuity of Operations Plan
DDP	Division of Disease Prevention
DURSA	Data Use and Reciprocal Support Agreement
FOIA	Freedom of Information Act
HHS	United States Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HIV	Human Immunodeficiency Virus
IRB	Institutional Review Board
ISO	Information Security Officer
ITRM	Information Technology Resource Management
NCHHSTP	National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention
NEDSS	National Electronic Disease Surveillance System
NIST	National Institute of Standards and Technology
OPGS	Office of Purchasing and General Services
ORP	Overall Responsible Party

PHI	Protected Health Information/Personal Health Information
PI	Personal Information
PII	Personally Identifiable Information
SDN	Secure Data Network
SODA	STD Surveillance, Operations and Data Administration
SSO	Site Security Officer
SSuN	STD Surveillance Network
STD	Sexually Transmitted Disease
TB	Tuberculosis
VDH	Virginia Department of Health
VH	Viral Hepatitis
VITA/NG	Virginia Information Technologies Agency/Northrop Grumman
VPN	Virtual Private Network

ATTACHMENT 3:

Verification of Receipt and Assurance of Key Requirements for DDP Personnel

Division of Disease Prevention (DDP) Security and Confidentiality Policies and Procedures
Verification of Receipt and Assurance of Key Requirements for DDP Personnel[14]
(Full time, part time, and wage employees, internal contractors, and students, interns)

If you handle, use, enter, or analyze DDP's confidential paper or electronic records or data, you must follow these requirements:

- Always protect and maintain security of state property you use (such as paper and electronic records, computers, flash drives, cell phones).
- Do not connect personal storage devices (such as non-state issued cameras, phones, MP3 players, flash drives) to state IT equipment/computers.
- Obtain supervisory approval before removing or transporting confidential information from DDP's agreed upon locations/offices.
- Transport confidential information in a locked briefcase or similar secure container.
- Use a state-issued IronKey™ flash drive if you must transport confidential electronic data.
    - Ensure data is encrypted or flash drive is stored under lock and key when not in use,
    - Keep flash drive in a separate location from your computer, and
    - Delete all data immediately after use.
- Store all confidential information in specified, locked file rooms.
- Return all confidential information to locked file rooms at end of workday.
- Do not store confidential information on the hard drive of your computer. It may only be stored on the Division network in designated folder locations.
- Collect, share, and transport the minimum confidential information necessary to conduct your work.
- Whenever possible, code information to avoid use of disease specific or client identifying information.
- Immediately report any known or suspected confidentiality breach to your immediate supervisor.
- No confidential information should be transmitted via email.
- Send mail in manner that does not allow confidential contents to be revealed.
- Faxes containing confidential information must only be sent to, or received at secure locations.
- Do not disclose confidential information over the telephone without first confirming the recipient is allowed access to the information.
- Access to all DDP databases requires completion of the Division's Database Access Request Form.
- Make every effort to ensure that confidential data is removed from PCs prior to surplus.
- Photography or video is not allowed in the Division's secured areas, unless it is necessary for business purposes and approved by your supervisor.

Your signature below indicates that:

- You have read the Security and Confidentiality Policies and Procedures in its entirety,
- You have read and understand these key requirements, and
- You have discussed any content you do not understand with your supervisor.

Name *(print)*:_____**Signature:**_____**Date:**_____

Supervisor's Signature:_____**Date:**_____

[14]This one-page document summarizes key attributes of the Security and Confidentiality Policies and Procedures. It is not inclusive of all Security and Confidentiality Policies and Procedures requirements.

Verification of Receipt and Assurance of Key Requirements for Non-DDP Personnel

Division of Disease Prevention (DDP) Security and Confidentiality Policies and Procedures
Verification of Receipt and Assurance of Key Requirements for Non-DDP Personnel[15]
(External contractors, service providers and data recipients)

If you handle, use, enter, or analyze DDP's confidential paper or electronic records or data, you must follow these requirements:

- Always protect and maintain security of state property you use (such as paper and electronic records, computers, flash drives, cell phones).
- Do not connect personal storage devices (such as non-state issued cameras, phones, MP3 players, flash drives) to state IT equipment/computers.
- Obtain DDP approval before removing or transporting confidential information from agreed upon locations/offices.
- Transport confidential information in a locked briefcase or similar secure container.
- Use an approved IronKey™ flash drive if you must transport confidential electronic data.
    - Ensure data is encrypted or flash drive is stored under lock and key when not in use,
    - Keep flash drive in a separate location from your computer, and
    - Delete all data immediately after use.
- Store all confidential information in specified, locked filing locations.
- Return all confidential information to locked file locations at end of workday.
- Do not store confidential DDP information on the hard drive of your computer.
- Collect, share, and transport the minimum confidential information necessary to conduct your work.
- Whenever possible, code information to avoid use of disease specific or client identifying information.
- Immediately report any known or suspected confidentiality breach to your immediate supervisor, DDP contract monitor and the DDP director.
- No confidential information should be transmitted via email.
- Send mail in manner that does not allow confidential contents to be revealed.
- Faxes containing confidential information must only be sent to, or received at secure locations.
- Do not disclose confidential information over the telephone without first confirming the recipient is allowed access to the information.
- Make every effort to ensure that confidential data is removed from PCs prior to surplus.
- Avoid photography or video in office locations that involve DDP confidential data, unless it is absolutely necessary for business purposes and approved by your supervisor(s).
- If you are a recipient of data from DDP, you will ensure that all data stewardship activities are handled according to the signed Data Request and Data Recipient Agreement forms.

Your signature below indicates that:

- You have read the Security and Confidentiality Policies and Procedures in its entirety,
- You have read and understand these key requirements, and
- You have discussed any content you do not understand with your supervisor.

Name *(print)*:_____Signature:_____Date:_____

Supervisor's Signature: _____ Date: _____

If employed external to DDP, identify your employer or affiliation: _____

_____

[15]This one-page document summarizes key attributes of the Security and Confidentiality Policies and Procedures. It is not inclusive of all Security and Confidentiality Policies and Procedures requirements.

ATTACHMENT 4:

Incident Handling Summary Procedures for Suspected Confidentiality Breaches

Summary of Incident Reporting Steps

1. Notify your immediate supervisor and the Site Security Officer (SODA Director) of the suspected incident as soon as it is discovered. Do not wait to report a potential loss, theft, or misplacement of confidential information in order to conduct an individual assessment of the incident.
2. Complete the Incident Response Form (Attachment 5) and give to your immediate supervisor. If IT equipment was lost or stolen, include the VITA program identification number (NG tag number).
3. Gather any/all documents that relate to the suspected incident.
4. Your unit manager will direct you to complete the VDH Client Safety Event Reporting Form based on Division management's assessment.
5. If a breach has definitively been identified, VDH management (Office of Epidemiology, Office of the Commissioner) must be notified first via Division management. The Security Officer for NCHHSTP, Ralph Vaughn, as well as the CDC Program Contact (Project Officer) must be notified within an hour of identifying the breach.

Preventative Measures

LOSS OR THEFT

- All hard copy documents must be transported within secured briefcases.
- Staff must have their contact information (name, phone number, e-mail) on their secure briefcases in case of being lost. Avoid use of working titles that would provide an indication of what the briefcase may contain.
- Only patient information necessary for the specific field-related work for that day should be transported outside of the office. Protected Health Information (PHI) that can be linked or used collectively to infer a disease condition must be removed. Disease coding (i.e. 200,300,700) should be used instead of disease names as needed.
- All confidential information should be returned to the secured location within the office at the end of each workday.
- Prior supervisor approval must be obtained when out of town travel or some other reason precludes returning confidential information on the same day. Supervisory approval for possession of confidential information within the field and/or taken home must be documented.
- The names of patient's hard copy paperwork that is taken out of the office must also be documented.
- Original forms of all paperwork should never leave the office. If copies must be used, staff must have relevant PII removed from the files.

IT EQUIPMENT

- If there is an incident involving IT equipment, the SSO must notify the Information Security Officer (ISO).
- Staff are responsible for ensuring the appropriate encryption software is installed on their laptops at all times. When a computer is refreshed or replaced it is the user's responsibility to make certain reinstallment of the software takes place.
- No confidential information, such as personnel data or PHI, should be stored on hard drives.

E-MAIL

- If an e-mail is received containing confidential information the user should notify their immediate supervisor of the possible e-mail breach right away.
- Staff should never forward or reply any e-mail containing PHI. If it was sent by an outside source, notify the sender of the incident by sending a new e-mail back.

- After notifying the sender, the user should immediately delete the e-mail from their “Inbox” and again within “Deleted Items”.
- Request sender to delete e-mail from all known potential places it could reside on their computers as well.

MAIL

- See the Procedure for Mailing Confidential Patient Information (Attachment 8)
- Staff must report any incoming or outgoing confidential mail that is delayed, lost, damaged or misdirected immediately to their supervisor.
- Staff must report any incoming mail that is known to have been delayed more than 5 business days.

ATTACHMENT 5:

Created: April 9, 2012

Incident Response Form

Immediately report a known or suspected incident, such as a violation of confidentiality or security. Complete the following information and submit to your immediate supervisor. The supervisor shall provide this documentation to the SSO (SODA Director) for audit purposes and notify the ORP (Division Director) of the incident.

Name of person reporting the incident: _____

Person who discovered the incident: _____

Date & Time incident was discovered: _____

Nature of the incident:

_____

_____

_____

Name of system and possible interconnectivity with other systems:

_____

Description of information lost or compromised:

_____

_____

_____

Storage medium from which information was lost or compromised:

_____

Controls in place to prevent unauthorized use of the lost or compromised information:

_____

_____

Person(s) and date contacted regarding the following:

1. VDH Leadership: _____
2. VDH OIM: _____
3. CDC ISSO/Program Contact: _____

Recommendations/Actions Taken (or to be taken): _____

_____

_____

Number of individuals potentially affected: _____

Was law enforcement contacted? _____

Signature: _____ **Date:** _____

ATTACHMENT 6: Created: 2002

Data Request Form

Requests for non-routine data, including any request for Division data sets, data matches or patient identifying information, must be submitted in writing to the Director of STD Surveillance, Operations and Data Administration for data release consideration. Clear explanation should be provided regarding proposed data needs. Submission of this request does not guarantee approval and/or release of Division of Disease Prevention data.

Submission Date: _____/_____/_____

Requestor: _____ Phone: _____-_____-_____

Title: _____ Fax: _____-_____-_____

Organization: _____ E-mail: _____

Purpose of Request:
_____
_____
_____
_____

Data Requested: [include timeframe(s), disease (s), demographics, etc]:
_____
_____
_____
_____

Data Use Methodology [if a research study/project, attach complete study design proposal]:
_____
_____
_____
_____
_____

Description of Data Protection Mechanisms [staff accessibility, electronic security, locks, etc]:
_____
_____
_____

At the conclusion of this project, the data will be: *(check one)*
☐Returned to the Division of Disease Prevention
☐Destroyed
Method*:*
_____
_____

_____
Signature of Requestor

cc: Data Recipient
Director of STD Surveillance, Operations and Data Administration

ATTACHMENT 7:

Data Recipient Agreement

The undersigned hereby agrees to the following terms and conditions relating to any data requested of the Virginia Department of Health Division of Disease Prevention:

A. The information obtained through this data request will be used only for surveillance of treatment, care and/or disease trends, prevention strategies or for statistical purposes in medical and health research.

B. No data shall be released or published by the data recipient in any form potentially identifying a particular individual, physician, hospital or other reporting source. Data subsets without personal identifiers must comply with confidentiality guidelines based on data cell size as approved by the Division of Disease Prevention.

C. By signing this agreement the data recipient agrees to abide by the Division of Disease Prevention's Security & Confidentiality Policies and Procedures.

D. Any identifying information in this data request shall not be used as a basis for legal, administrative, or other actions that may directly affect those particular individuals or establishments as a result of their specific identification in this project.

E. Information obtained through this request shall not be distributed to anyone else, including subcontractors and third-party analysts. The data shall not be used for any project other than the intended use specified in the data request.

F. Unless specified and approved through the original proposal, no "follow-back" investigations to obtain additional information from physicians, hospitals, or patients shall be undertaken.

G. All data received from the Division of Disease Prevention shall be returned to the Division or disposed of by an approved method at the end of the project. The data recipient shall state the method of return or disposal prior to receipt of the data. Written confirmation of data destruction is required and should be sent with attention to the Director of STD Surveillance, Operations and Data Administration at 109 Governor's Street, Richmond, VA 23219.

H. If the requestor of data for a given project changes, the organization receiving the data shall inform DDP, as outlined on the Data Request Form.

I. Any suspected or confirmed breach of data confidentiality or security shall be immediately reported to the Director of the Division of Disease Prevention.

J. Draft versions of all work products shall be sent to the Division of Disease Prevention for review and approval prior to any distribution. Sufficient time should be allotted to allow for review and comments prior to distribution.

K. A copy of all final work products resulting from use of the data shall be sent to the Division of Disease Prevention prior to or at the time of distribution.

As a recipient of data from the Virginia Department of Health Division of Disease Prevention, I agree to abide by the above stipulations.

Signature: _____ **Date:** _____

Organization: _____

ATTACHMENT 8:

Created: May 16, 2012

Procedure for Mailing Confidential Patient Information-Incoming

DDP programmatic forms **HIV Counseling, Testing, and Referral Forms, Interview Records, Field Records, Sexually Transmitted Disease Surveillance Network (SSuN), HIV Incidence, pediatric tracking, electronic disease notification printouts, and Report of Verified Case of Tuberculosis,** etc.] containing confidential patient information may be received via a secure mail system, provided the mailing is done in a confidential manner that meets or exceeds the following:

Use **two** envelopes when mailing forms regarding HIV, AIDS, STD, TB, and Newcomer Health:

- Forms shall be placed inside the "first" or inner envelope and securely sealed with packaging tape. The envelope must protect contents from being read or viewed, and a regular manila envelope will meet this requirement. The number of forms placed within the envelope shall not exceed 25 or 1 inch stacked. The total number of forms being sent shall be documented in the upper right corner on the outside of the inner envelope.

- The "second" or outer envelope must be made of a material that is tear-, puncture-, and moisture-resistant, such as Tyvek. DDP will provide these envelopes for use by HIV testing sites, SSuN sites, and staff performing disease intervention activities.

- The recipient and sender name and address shall be placed on the inner envelope. DDP will provide local health districts, HIV testing sites, and SSuN sites with United Parcel Service (UPS) mailing labels for "return service." The UPS label shall be placed on the "second" or outer envelope. Double addressing gives an additional level of security that the envelope will reach the intended person/address.

- The frequency of mailing shall be at least weekly. It is suggested that mailings be combined where activities are occurring in multiple clinics at the same location if the volume is less than 25 forms. If UPS service has not been established, you can call 1-800-PICK-UPS® (1-800-742-5877), a fee may be charged.

- Sender shall track the envelope to verify delivery of your mail

Procedure for Mailing Confidential Patient Information-Outgoing

DDP programmatic forms [**HIV Counseling, Testing, and Referral Forms, Interview Records, Field Records, Sexually Transmitted Disease Surveillance Network (SSuN), HIV Incidence, pediatric tracking, electronic disease notification printouts, and Report of Verified Case of Tuberculosis,** etc.] containing confidential patient information may be sent via United Parcel Service (UPS), provided the mailing is done in the following manner:

Use **two** envelopes when mailing confidential information regarding HIV, AIDS, STD, TB, and Newcomer Health:

- Forms shall be placed inside the "first" or inner envelope and securely sealed with packaging tape. The envelope must protect contents from being read or viewed, and a regular manila envelope will meet this requirement. The number of forms placed within the envelope shall not exceed 25 or 1 inch stacked. Document the total number of forms being sent in the upper right corner on the outside of the envelope.

- The "second" or outer envelope must be made of a material that is tear-, puncture-, and moisture-resistant, such as Tyvek.

- The recipient and sender name and address shall be placed on the inner envelope. The UPS mailing label, "signature required", shall be placed on the "second" or outer envelope. Double addressing gives an additional level of security that the envelope will reach the intended person/address.

- Sender shall track the envelope to verify delivery of your mail.

ATTACHMENT 9:

Fax Cover Sheet

Virginia Department of Health
Division of Disease Prevention
P.O. Box 2448
Richmond, Virginia 23218

Physical Address: 109 Governor Street, 3rd floor, Richmond Virginia 23219

Main Office Number: (804) 864-7964 Main Office Fax Number: (804) 864-7983

FACSIMILE

DATE: _____

TO: _____

FAX NUMBER: _____

PAGES (including cover sheet): _____

FROM: _____

☐ *Urgent* ☐ *For Information / Review* ☐ *As Requested* ☐ *Reply Requested*

_____

Comments/Additional Information

Confidentiality Notice

The document(s) accompanying this fax transmission may contain health information that is legally privileged. This information is intended only for the use of the individual or entity named above. The authorized recipient of this information is prohibited from disclosing this information to any other party unless required to do so by law or regulation and is required to destroy this information after its stated need has been fulfilled. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken related to the contents of these documents is strictly prohibited. If you have received this information in error, please notify the sender immediately and arrange for the return or destruction of these documents.

ATTACHMENT 10:

Created: July 3, 2012

Procedures for Running Virus Scan on IronKey Flash Drives (when used in conjunction with non-COV equipment)

Purpose: According to Virginia Information Technologies Agency (VITA) and Virginia Department of Health (VDH) Information Technology policies, it is inappropriate to connect Commonwealth of Virginia (COV) equipment, including mobile devices, to non-COV equipment. Various Division of Disease Prevention (DDP) programs also require the transfer/transport of protected health information (PHI) data files with non-COV partners for routine business operations. Examples of such partners include universities, community-based and/or not for profit organizations and/or healthcare providers.

If a secured electronic mechanism for data transport is currently unavailable for use with a non-COV partner, use of a COV-approved IronKey encrypted flash drive may be considered allowable, in order to comply with the VDH Confidentiality Policy. The IronKey product uses a password-protected drive to encrypt the file during physical transport between non-COV partners and DDP-specific computers and/or secured, network folder locations.

Any DDP program that requires use of an IronKey data transfer process should provide a description of the business process, COV file storage location and affiliated non-COV partners to the Director of STD Surveillance, Operations and Data Administration, who will work with the VDH Information Security Officer to receive approval for IronKey use. The DDP will review other methods of secure transport; as such mechanisms become available, and based on agency direction.

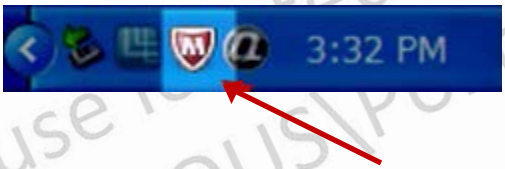
Upon approval, the following steps shall be followed to ensure virus scans are performed appropriately. Routine virus scans absent of any known viruses can proceed with normal data downloads and subsequent removal of such data files from the IronKey flash drive. If the routine scan detects a virus, program staff should immediately cease all related activities associated with the data file transfer process and inform their supervisor for appropriate follow up activities.

Steps to Run McAfee Virus Scan on IronKey Flash Drives

1) Insert the IronKey flash drive, into a USB port on your PC. This should be the IronKey device with a data file that needs to be uploaded to a Division of Disease Prevention server location.

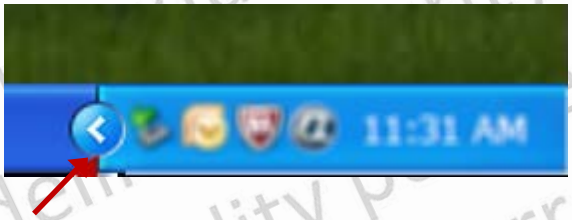
2) Unlock the IronKey flash drive using your standard password-protected procedure. DO NOT open any files on the IronKey at this time.

3) Open the McAfee Virus Program, located at the lower right side of your task bar in the Status Tray.



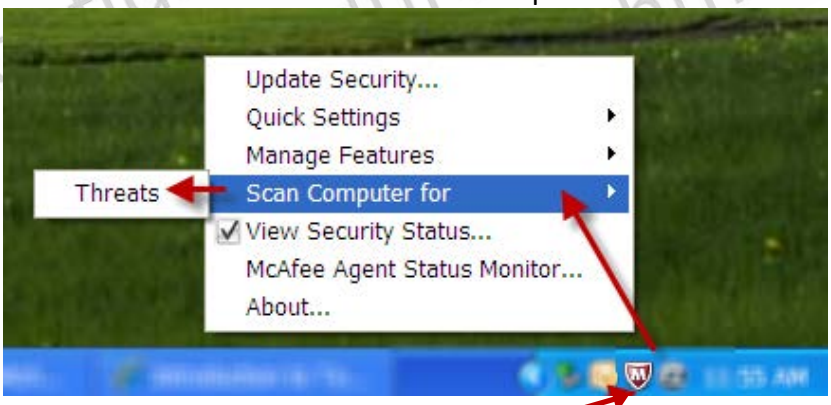
McAfee Virus program icon

NOTE: If you do not see the McAfee icon on your task bar in the status tray, then select the < arrow/button to expand and show the hidden icons.



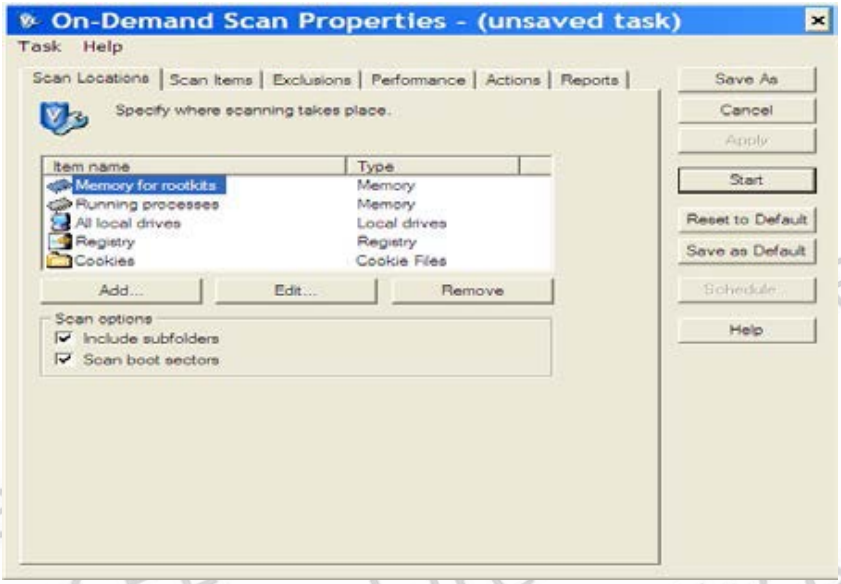
Expand button (select to view all icons on this task bar)

4) Right click on the McAfee icon and scroll to "Scan Computer for…" and "threats".

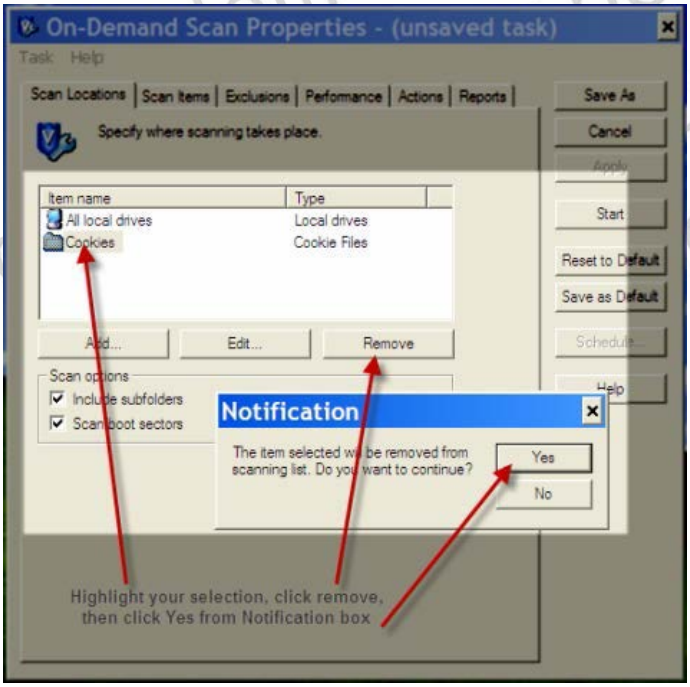


Open McAfee: select Scan Computer for; Threats

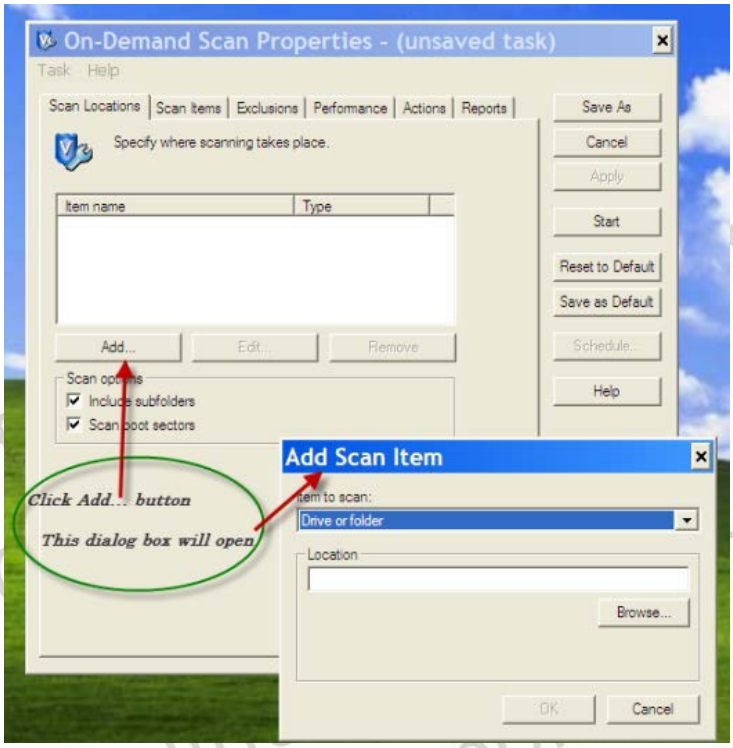
The Scan console should appear as follows, with a number of items showing in the "Item name" list under the "Scan Locations" tab.



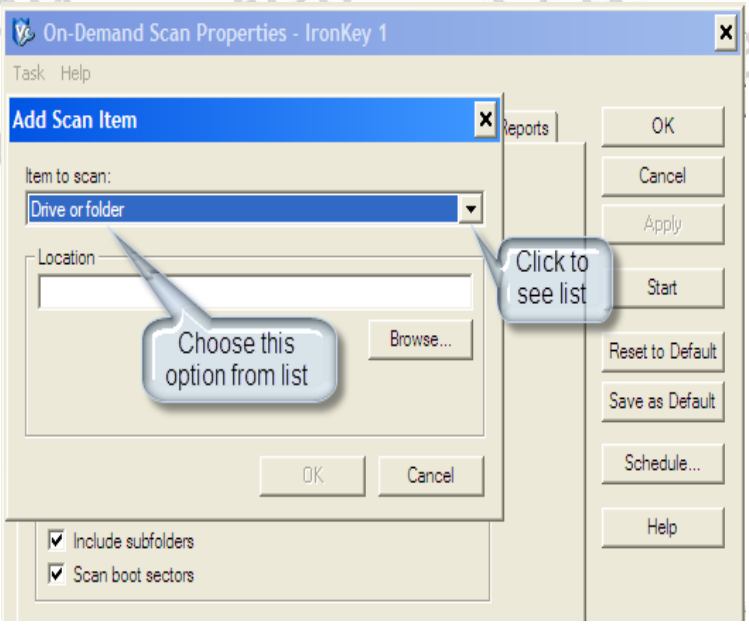
5) Create a new Task to run scans on the IronKey flash drive by doing the following: First, remove each item on the default list (shown above). Do this by highlighting each default item and clicking the "Remove" button. Then select "Yes" when the Notification dialog box opens. Repeat this step until all items have been cleared from the "Item name" list. NOTE: Be sure the default list is empty before proceeding to step 5.



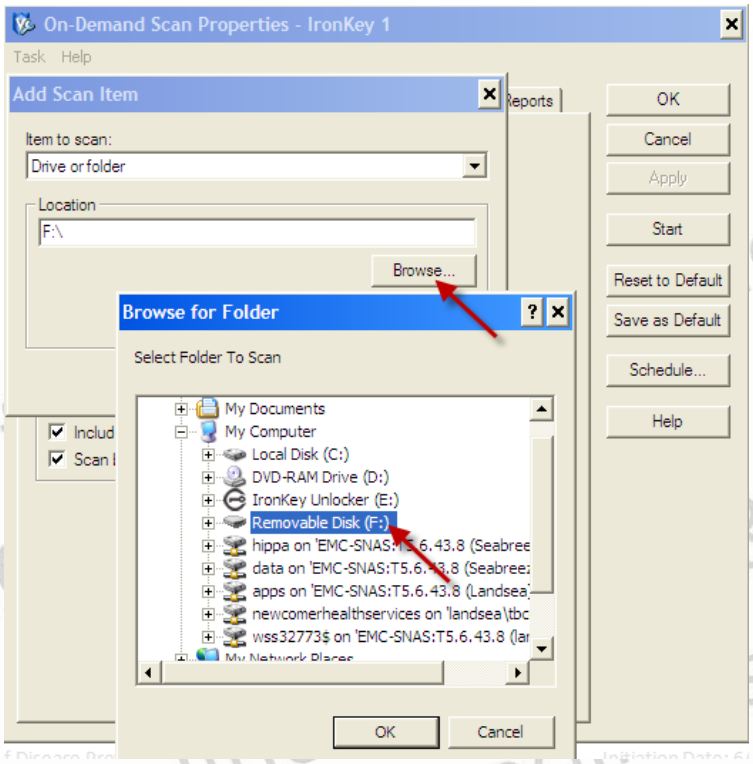
6) Click “Add”. Another dialogue box called “Add Scan Item” will appear.



7) In the “Add Scan Item” box, use the drop down arrow and select ‘*Drive or folder”*.



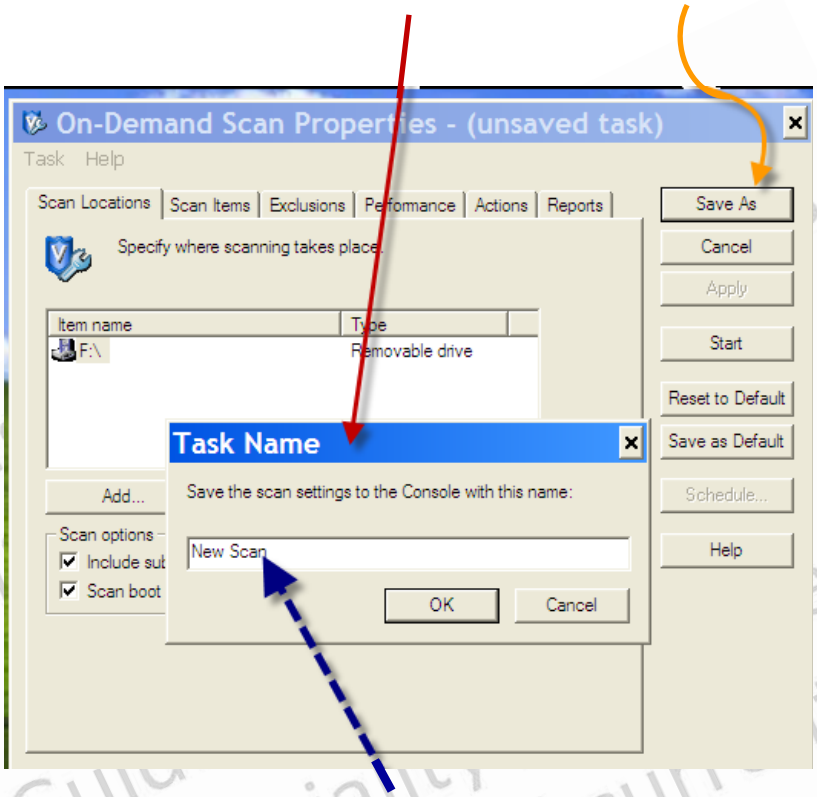
8) Click “Browse”. Then, select the IronKey flash drive location. In the image below, it is the (F:) drive. Click OK and the drive letter appears in the location box. NOTE: The IronKey may use a separate drive as the IronKey Unlocker (see (E:) drive below). If so, repeat this step to include both drives as locations to scan.



9) After all necessary drives have been added, Click OK again. The Drive(s)/folder(s) selected now should appear under “Scan Locations”.

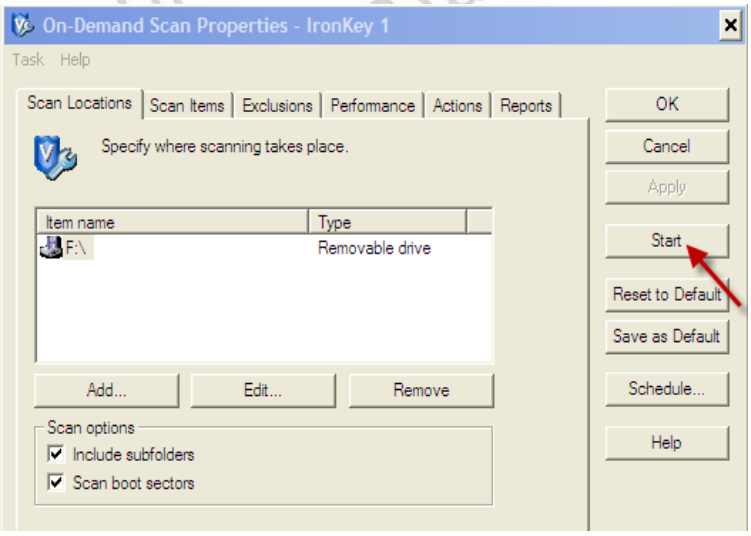
10) Click “Save As” and the Task Name dialogue box will appear. Type in the name you wish to call the task, i.e. “IronKey”, and click “ok”.

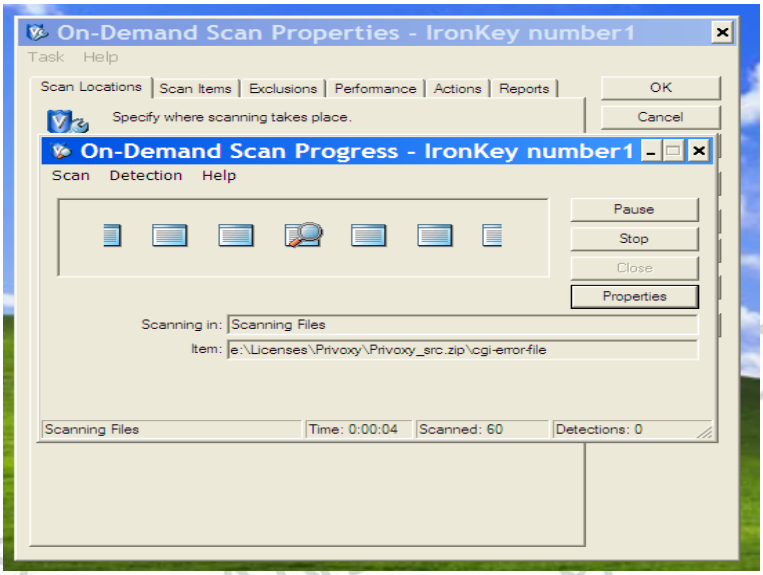
Click as Save As
(The Task Name dialog box will open)



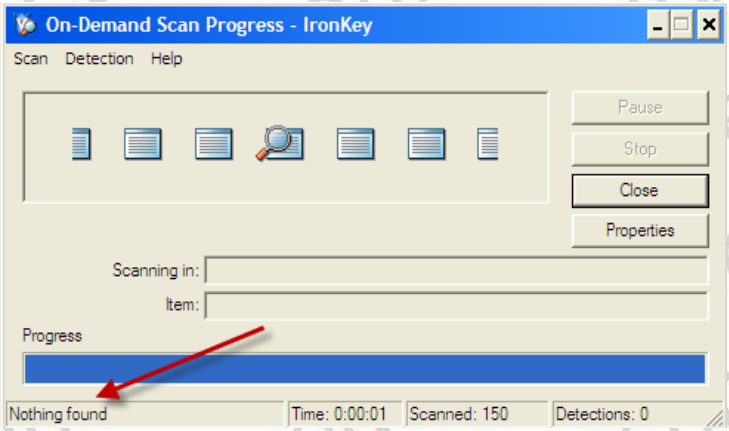
This is where you will type in the name you've selected for your IronKey scan task. Giving it a name will allow you to choose this, as a short cut, to perform the scan task each time you insert your flash drive.

11) Click "Start" to begin scanning the selected drives. The second image below shows the scanning in progress.





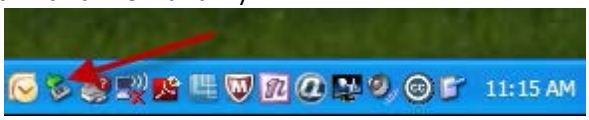
12) Once scanning is complete, you will hopefully see that no viruses were found. If viruses are found, contact your supervisor and DO NOT upload any files! (see page 1, under "Purpose").

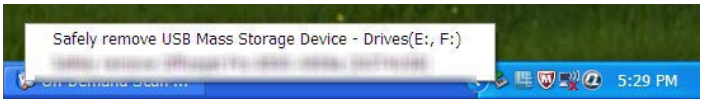


13) Click "Close" if there are no viruses identified and proceed with upload of file(s).

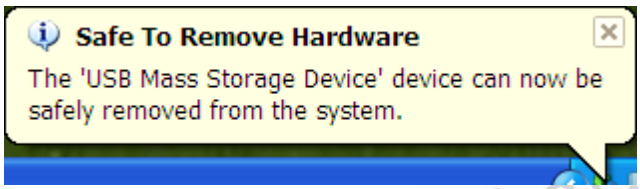
Safely Removing the IronKey Flash Drive

14) To remove the IronKey flash drive, select the Safely Remove Hardware button on the Status Tray of your taskbar. Select the item you wish to remove by clicking on the description. (In this example, the IronKey flash drive appeared with drive E and F.)





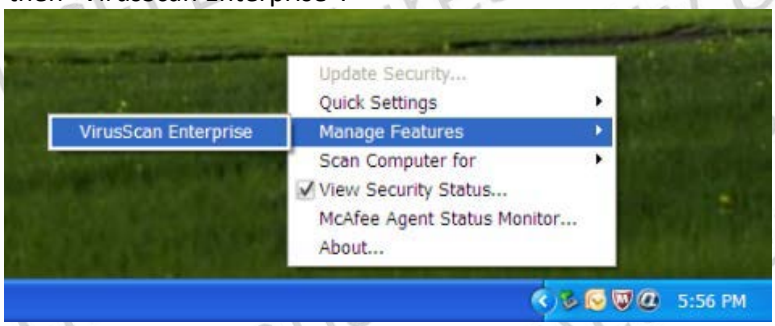
15) A dialog balloon pop up indicating it is safe to remove hardware should appear. The IronKey can now be safely removed from the USB port.



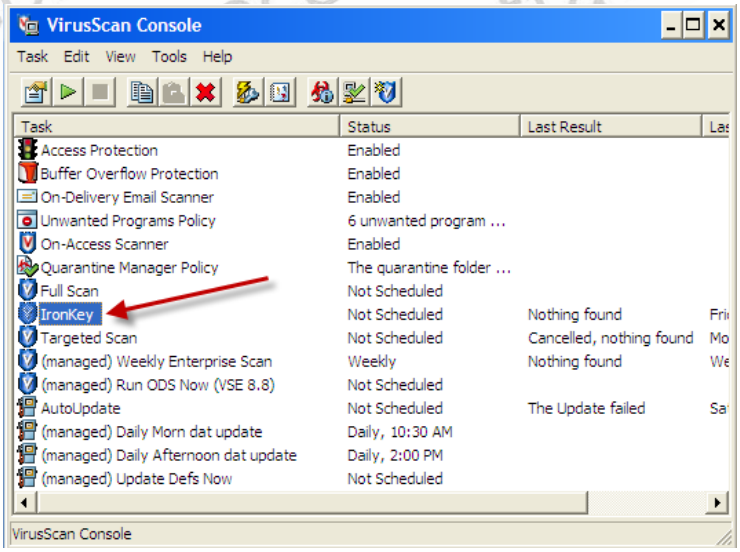
Performing Repeat Scans Using the IronKey Flash Drive

16) Insert the IronKey with the file(s) for upload.
Division of Disease Prevention Initiation Date: 6/11/2012 7

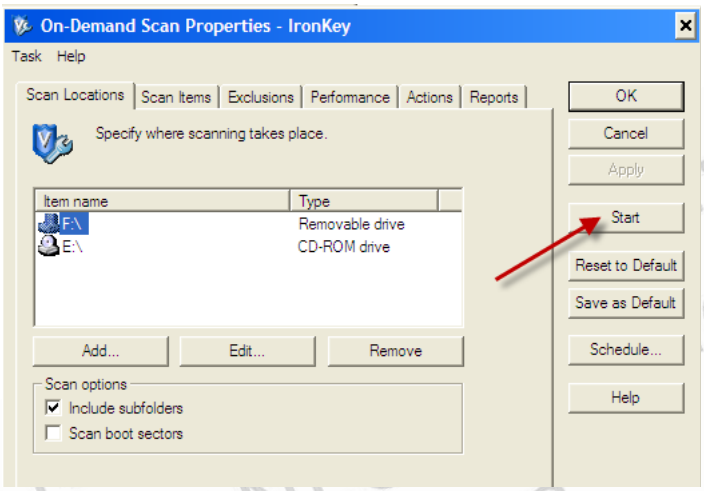
17) Open McAfee by clicking the icon in your status tray (on the toolbar/status tray) and choose "Manage Features", then "VirusScan Enterprise".



18) The VirusScan Console box will open. Choose the desired scan you wish to run. In the example below, the Targeted Scan was saved as "IronKey".



19) Double click the desired scan (i.e. IronKey). The image/box below will be displayed. Click “Start” to begin the scan.



20) Follow Steps 12-13 above.

ATTACHMENT 11: Created: June 29, 2012

IronKey Flash Drive Program Operation Activities

Date Submitted:

Work Unit Name: ex. HIV Surveillance Program

Name of DDP Submitter: ex. Jane Doe

Name of Business Process: ex. VCU HIV virology lab transfer

Type of Data Involved: ex. Positive HIV/AIDS laboratory results

Name of non-COV Entity: ex. VCU Health System (virology lab)

Contact Information at non-COV Entity: Name, Position, Telephone, E-mail

Occurrence Interval: ex. Every Friday, first Monday of the month, quarterly, etc.

COV File Storage Location: ex. I:\SURVEILLANCE\MCV_CD4_VL\2012

Business Process: Describe the programmatic necessity and procedures involved.

List any alternative file transfer possibilities:

List all VDH personnel that may handle the IronKey flash drive for this activity:

Approval:

DDP Program Area Signature:_____ **Date:** _____

DDP Site Security Officer Signature: _____ **Date:** _____

OIM Signature: _____ **Date:** _____

Denial:

DDP Site Security Officer Signature: _____ **Date:** _____

OIM Signature: _____ **Date:** _____

Reason for denial:

ATTACHMENT 12:

Created: August 7, 2012

Electronic Media Mailing Form

Date Submitted: _____

Work Unit Name: _____

Name of DDP submitter: _____

Type of Media to be mailed: _____

Type of Data Involved:_____

Name & Address of mail receiver: _____

_____

_____

Estimated Arrival Time:_____

Contact Information of mail receiver:_____

_____

_____

Approval:

Division Management Signature: _____**Date:**_____

Information Security Signature: _____ **Date:**_____

Denial:

Division Management Signature: _____**Date:**_____

Information Security Signature: _____**Date:**_____

Reason for Denial:

ATTACHMENT 13:

Procedures for Establishing and Managing Network Domain and DDP Database Access Accounts

A. COV Account Requests

1. All staff (FTEs, wage, internal and external contractors, volunteers and interns) that requires access changes (new accounts, edits, deletions, disabling) to any of the division's network files and/or require an email account must have a Commonwealth of Virginia (COV) Account Form completed. Instructions for how to complete the COV Account Form are available for staff use at M:\MISCELLANEOUS\Policies Procedures & Guidelines\COV Account Request Form. Supervisors should ensure COV submissions are handled in a timely manner regarding staff accounts.
2. Submissions are automatically emailed to the Office of Epidemiology (OEPI) COV account approver. The DDP SODA director serves as the approver for all OEPI divisions, except Radiological Health.
3. Approved submissions are emailed to VCCC by the OEPI approver. Questions or denials regarding specific access that appears inappropriate is discussed with the submitter/manager.
4. Copies of submissions are retained by the approver for audit and tracking purposes.
5. VCCC emails the submitter, manager and approver upon completion of the request.

Additional information pertaining to COV account network groups/folders and VPN is listed below:

DDP Network Groups and/or Folders

- The Division maintains numerous network groups/folders to ensure that programs or work units have specified network accessibility, as well as restricted network access requirements, as needed. Each network group has privileges established as either Read Only (RO) or Read Write (RW). Network folders are typically named the same as group titles. Business requirements for additional folders should be discussed with the SODA director, in order to ensure proper requests via the COV form listed above.

Virtual Private Network (VPN) Access

- The COV form is used to request access to the Commonwealth's Virtual Private Network (VPN). Once an employee is added to the VPN network, he/she must also determine if the VPN Client is installed on their PC.
- Staff can determine if the client is installed by going to START\Programs\CISCO VPN Client). If the CISCO VPN Client does not appear, a VCCC ticket should be created to request installation.
- Two VPN options exist - Single Factor Authentication and Dual Factor Authentication.

Single Factor Authentication

- This is the level that most approved staff will use. It allows for access to the COV domain remotely, as if the user is logged in at their respective office location.

Dual Factor Authentication

- This is the level used by staff who require access to the back end of a server. Typically, this is only necessary for staff who perform certain database management functions. There is also a one-time cost for the token required for COV access. This can be procured through routine procurement channels. However, requests for tokens should not be made unless DDP management has determined it to be a justifiable business need of the position.

B. Remote Email Accessibility

- Access to email from remote locations can be achieved via two mechanisms:

1) use the VITA Outlook Exchange web site (https://webmail.vita.virginia.gov/owa/auth/logon.aspx)
2) use an established VPN connection.

C. DDP Database Access Form Requests

1. All staff (FTEs, wage, contractors, volunteers and interns) that requires access changes to any of the Division's databases must complete the Database Access Request Form.
2. The form is available as an attachment to the DDP Security and Confidentiality Policies and Procedures, as well as in hard copy format via a file box labeled Database Access Request Form, located outside office 328. NOTE: If a copy is printed electronically, be sure to include both pages and print the form front and back on a single sheet of paper.
3. The supervisor completes the staff's information on the form, as well as the database(s) and access needs requested.
4. The form is routed to the SODA director for request approval/denial. Questions regarding specific access to systems that appears inappropriate are discussed with the submitting supervisor. Denied requests are discussed with the submitting supervisor.
5. Approved forms are routed to appropriate data managers for account creation and follow up with the respective employee to provide temporary passwords, etc.
6. Completed forms are returned to the SODA director for audit and tracking purposes.

D. Maintenance of Account Records

1. All COV and DDP Account forms are stored alphabetically by the SODA director.
2. Approved requests are printed and stapled on the top of any other existing account request approvals for each employee.
3. Paperwork for employees ending employment with DDP, or other OEPI divisions, are removed from the active files and placed in a separate folder for records retention processing.

E. Accessing Non-DDP Data Systems or Applications

1. DDP-specific data systems are included on the request form above (Part C.). All other systems require separate procedures/forms and must follow processes from the respective work area, division or office. Examples include:

   WebVision – Office of Information Management and HealthIT

   F&A (Financial & Administration) - Office of Information Management and HealthIT

   VEDSS – Division of Surveillance and Investigation

   CIPPS (Commonwealth Integrated Payroll/Personnel System) – Department of Accounts

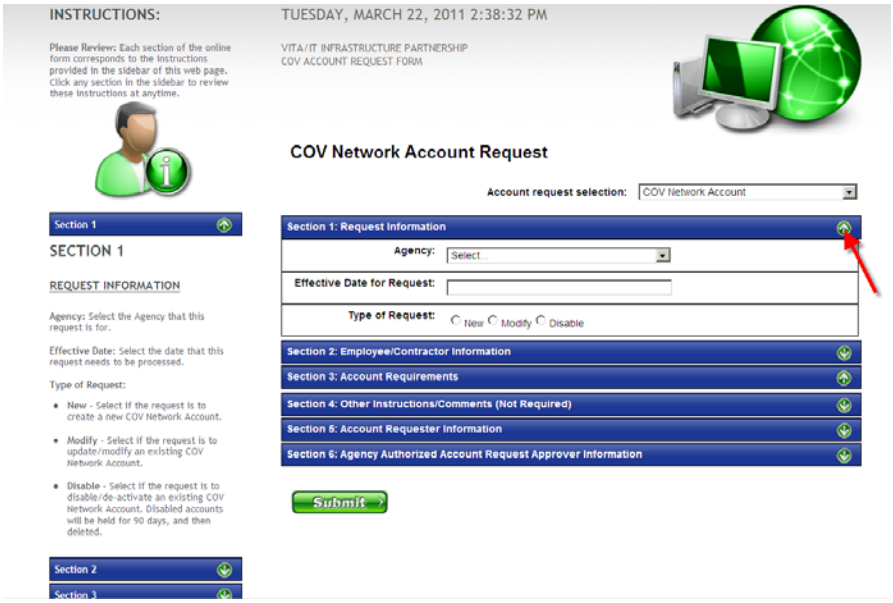
   PMIS (Personal Management Information System) – DHRM

ATTACHMENT 14:

Steps to Completing the COV Account Request Form

1) Click on the following URL: https://esupport.virginia.gov/accountrequest/. This will take you to the following web page. Click on the drop down list (see red arrow below) to choose the type of activity being requested. Most requests will be for things such as COV Network Account, Folder/Share Access or Distribution Lists.

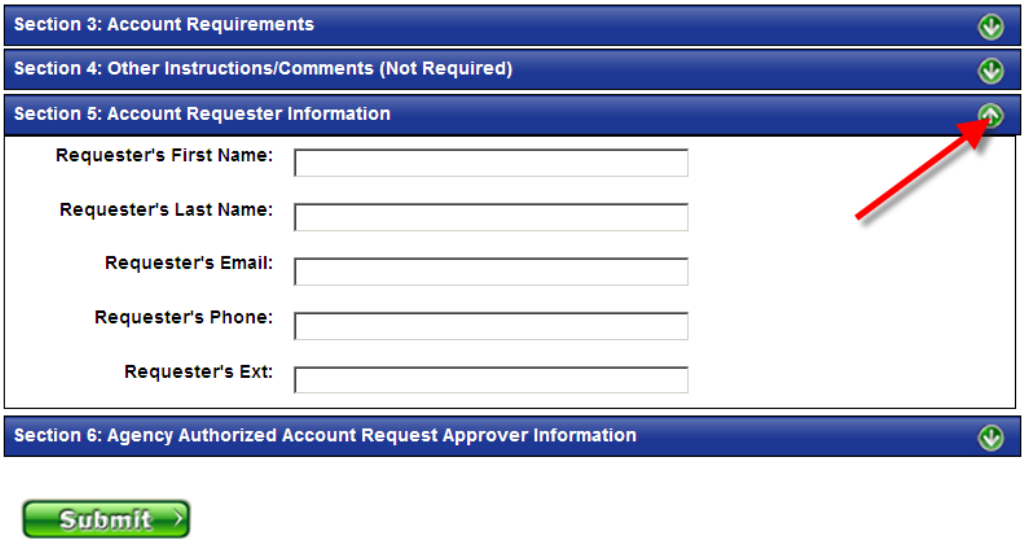
2) The form will be shown as below. Click on each section to expand the data options. Note that the left hand side will expand to provide helpful information and definitions for the data elements within each section. Complete sections 1-4 (section 4 is optional).



Section 2 is the Employee/Contractor Information. This is the section where you will record the manager's information. The manager should be the actual supervisor of the employee/contractor (for OIM staff assigned to OEpi, the manager should be the appropriate OIM supervisor).

Section 3 is the Account requirements. This is where you will record the groups or shared folders for which access is needed. Be sure to record whether the person needs Read Only (RO) or Read Write (RW) privileges.

3) Section 5 is the Requestor information. This is the person sending the request, or for whom the form is being sent on behalf of. The person listed in this section is whom the email will appear to be sent from for approvals (although he/she may not have physically generated the email). For example, May Anne Wollman could generate a COV form with Dave Trump as the requestor and the information will appear as though Dr. Trump generated the form.

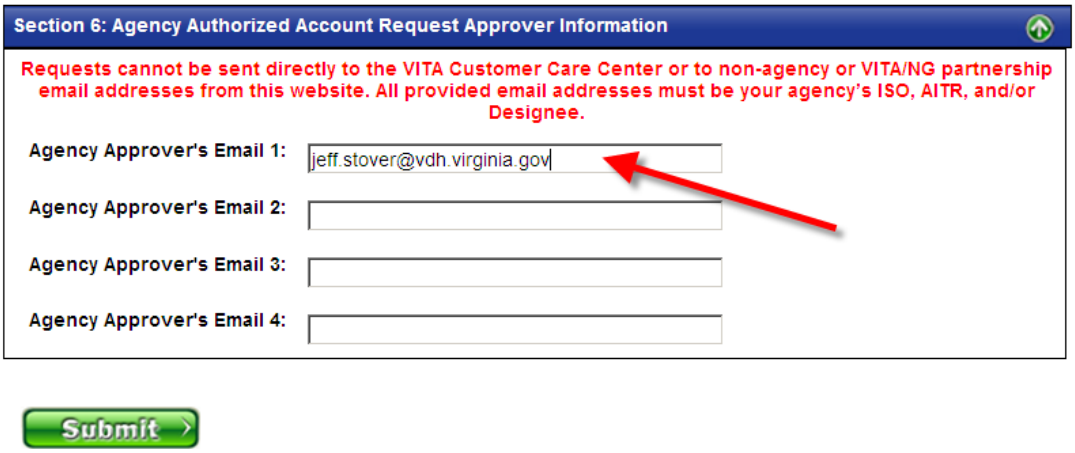


4) Section 6 is the Approver information. Jeff Stover is the designated approver for OEpi. Jennifer Loney will serve as the backup approver.

For OEpi employees/contractors, you should list approvers as follows:
Approver 1: jeff.stover@vdh.virginia.gov.
Approver 2: Jennifer.loney@vdh.virginia.gov

For OIM employees/contractors, you should list approvers as follows:
Approver 1: wes.kleene@vdh.virginia.gov
Approver 2: debbie.condrey@vdh.virginia.gov

**NOTE: Do not include supervisors in section 6. The VCCC only recognizes COV Account Approvers that have been identified and provided by each agency.

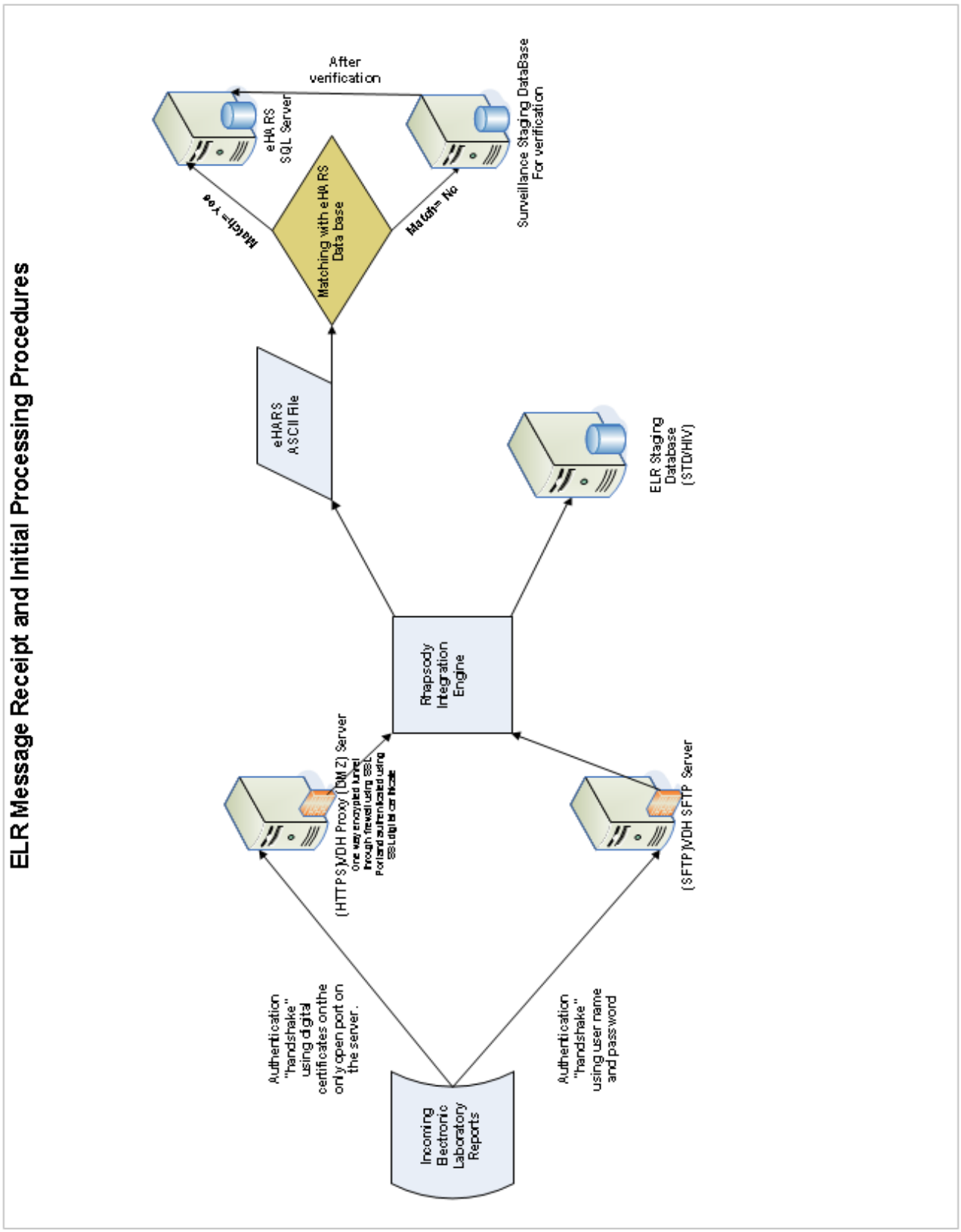


5) Click Submit and an email will be automatically sent to the approver(s) for review, approval and submission to VCCC. A Word document will be attached to the email with the form you completed. The email will also be copied to the requester.

6) Copies of all COV Account Request Forms will continue to be maintained for OEPI audit purposes or, as needed, for review of folder access privileges.

7) NOTE: Unless otherwise stated (as has been done by DSI), the approver(s) will assume that the requester has reviewed such requests with the appropriate manager. And, barring any necessary edits, the approvers will proceed with forwarding the requests to VCCC. Please let the above OEpi approvers know if your division has special circumstances requiring additional approvals after initial COV Account Form submission.

ATTACHMENT 15: Created: November 8, 2012



ATTACHMENT 16:

Created: December 13, 2012

Surveillance & Investigation Site Visit Procedures

The purpose of this policy is to standardize pre- and post-surveillance site visit practices to minimize the risk of confidentiality breaches, as well as to emphasize existing site visit data requirements, as per Division of Disease Prevention Security and Confidentiality Policies and Procedures. These procedures are mandatory and must be followed for each site visit.

1. Complete the appropriate program-specific Surveillance Site Visit (SSV) and the Patient Line List (PLL) forms prior to the visit date. NOTE: An alternate pre-existing PPL list can be used. The PLL should include only the minimum amount of information required to identify clients or to conduct the visit. Always use disease codes if possible, i.e. 350, 710, 900, 950, etc.
   The forms are located at the following locations:
   - STD Surveillance, Operations and Administration Staff
     File Location: M:\SODA\Site Visit Reports
   - HIV Surveillance Staff
     File Location: I:\Surveillance\Confidentiality Policy & Forms
2. Save the completed SSV and PLL files in the following program-specific locations:
   - STD Surveillance, Operations and Administration Staff
     File Location: M:\SODA\Site Visit Reports\Lab Visits
   - HIV Surveillance Staff
     File Location: I:\Surveillance\Confidentiality Policy & Forms\Staff Site Visits
3. Use the following naming conventions to save files in the folders listed in #2 above:
   - SSV file: (first letter of first name, first letter of last name, “underscore”, site visit date, “underscore”, SSV). Example: a site visit to be conducted on 12/1/2012 by Jane Doe would be saved as follows: JD_12012012_SSV.xls.
   - PLL file: (first letter of first name, first letter of last name, “underscore”, site visit date, “underscore”, PLL). Example: a site visit to be conducted on 12/1/2012 by Jane Doe would be saved as follows: JD_12012012_PLL.xls.

4. Provide a printed copy of the signed SSV and PPL forms for supervisory review, approval and signature prior to the visit date. Employees are not allowed to take any such data out of the office for a site visit without signed supervisory approval. Additionally, the completed SSV and PLL forms are not to be taken out of the central office, as these files contain reference to surveillance data, as well as patient identifiable information.
5. Supervisors shall review form requests for surveillance site visits on a daily basis and notify affected staff of approval/denial. Approved and signed hard copy forms shall be filed in the following locations:
    - STD Surveillance, Operations and Administration Staff

      Location:
    - HIV Surveillance Staff

      Location: eHARS file room SSV/PLL accordion file. This file is located in the first drawer of the surveillance file cabinet.
6. While in the field…
    - If return of confidential data to the office cannot be completed as scheduled, the employee must receive supervisory approval to retain the personally identifiable information outside of the central office location. Employees should carry relevant supervisory staff contact information when performing field visits to ensure approval is obtained in the event his/her immediate supervisor is unavailable.
    - If a suspected security breach occurs, employees must immediately report the incident to their supervisor and the site security officer. See section "Incident Handling for Confidentiality Breaches" within the Security and Confidentiality Policies and Procedures for additional guidance.
7. Upon returning to the office, the employee shall immediately retrieve the approved/signed SSV/PLL forms, perform "check-in" updates and provide the documents to the supervisor for final "check-in".
8. The supervisor completes the final "check-in" procedure as a priority activity and re-files the forms in a completion folder within the location specified in #5 above. Supervisors must document any unforeseen events involving staff possession of confidential information that

occurred in the field (e.g. additional overnight hotel stay, non-routine information taken to staff private residence, etc) and shall include this information with the SSV checklist approval documentation. These documents will be retained as Administrative Records, as per Library of Virginia Retention Policies.

NOTE: Refer to the Division's comprehensive documentation related to security and confidentiality on a routine basis to ensure compliance with all activities, including field visits.

ATTACHMENT 17:

Coordination of Care and Services Agreement

Place Agency Name Here:_____

COORDINATION OF CARE AND SERVICES AGREEMENT
PAGE 1 OF 2

I understand that different agencies provide different services and benefits, and that each agency must have specific information to provide services and benefits. By signing this form, I allow agencies to use and exchange certain information about me so it will be easier for them to work together efficiently to provide or coordinate these services or benefits.

1) I, _____am signing this form for the opportunity to receive coordination of services.
(Print Client's Full Name)

_____ _____
Client's address **Client's Date of Birth**

2a) Client Diagnosis:

☐ HIV/AIDS HIV/AIDS Diagnosis Date:_____

☐ Hepatitis C (HCV) Hepatitis C (HCV) Diagnosis Date:_____

2b) Current Gender of Client
- ☐ Male
- ☐ Female
- ☐ Transgender – M2F
- ☐ Transgender – F2M
- ☐ Transgender – Unspecified
- ☐ Declined
- ☐ Other, Specify:_____

2c) Client Race:
- ☐ American Ind./AK Native
- ☐ Asian
- ☐ Black/African American
- ☐ Native HI/Pac. Islander
- ☐ White
- ☐ Don't Know
- ☐ Declined

2d) Client Ethnicity:
- ☐ Hispanic or Latino
- ☐ Not Hispanic or Latino
- ☐ Don't Know
- ☐ Declined

3a) I allow the following confidential information about me to be shared (check all that apply):
- ☐ Contact information
- ☐ Medical Diagnosis
- ☐ Mental Health Diagnosis/Treatment
- ☐ Demographic Information
- ☐ Medical Appointments
- ☐ Substance Use Diagnosis/Treatment
- ☐ Financial Information
- ☐ Individual Services Plan
- ☐ Client's testing information
- ☐ Other:_____

Information in the boxes indicated above may be updated and shared with the providers indicated in **3b.** ☐ **Yes** ☐ **No**

3b) I consent that the information indicated in item 3a can be released for the following care arrangements (check all that apply) <u>as specified on page 2 of this form</u>:
- ☐ Medical Care Providers
- ☐ Other Core Medical Service
- ☐ Mental Health/Substance Use Services
- ☐ Medication Access
- ☐ Other Support Services

4) I may be contacted by the following methods (check all that apply):
- ☐ In person only, at this location: _____
- ☐ Postal Mail/Letter. Address, if different from above: _____
- ☐ Home Phone: _____ May we leave a message? (circle) YES NO
- ☐ Cell Phone: _____ May we leave a message/text message? (circle) YES NO
- ☐ Work Phone: _____ May we leave a message? (circle) YES NO
- ☐ Email: _____

5a) This agreement is effective: _____ **5b)** If revoked, check box, sign and date ☐ _____
(Date of Agreement) (**Sign and Date if revoking agreement)**

It is understood that this agreement for the **<u>coordination of my care services</u>** is valid for **<u>24 months</u>** from the agreement date.

In addition, it is understood that in order to assist in the coordination of my care, a health system navigator (HSN), or patient navigator (PN), or other type of linkage to care staff or personnel can attempt to contact me by the above-approved methods, in the event that I miss a scheduled medical or other type of appointment related to my HIV care.

I can withdraw this agreement at any time by informing all referred agencies. The listed agencies must stop sharing information after I inform them that my authorization has been withdrawn. I have the right to know what information about me has been shared, why, when, and with whom it was shared. If I ask, each agency will show me this information. I want all agencies to accept a copy of this form as valid consent to share information. If I do not sign this form, information will not be shared and I will have to contact each agency individually to give information about me that is needed. However, I understand that treatment and services cannot be conditioned upon whether I sign this agreement.

6) Signature(s) of Client or Authorized Person(s)_____**Date:** _____

7) Person Explaining Form: _____
(Name) **(Agency)** **(Phone Number)**

Place Agency Name Here:_____

COORDINATION OF CARE AND SERVICES AGREEMENT
PAGE 2 of 2

SECTION A: To be filled out by agency who originated the form.

1a) Originating Agency Representative's Name:_____ **Secure Fax:**_____ **Phone:**_____

1b) Client:_____ **1c) Client Date of Birth:** _____
(Print Client's Full Name)

1d): Name of Organization(s) Client Being Referred to: _____

_____

_____

_____

SECTION B: To be filled out by medical provider or linkage personnel who will be linking the client to care after receiving referral from the original agency. Please complete Section B and fax this information back to the agency who originated this form. Please be sure to use a fax cover sheet and ensure that all fax lines are secure.

2b) Name of Person Linking Client to Care:_____ **2c) Agency Name:**_____

2d)Telephone and Secure Fax Number of Person Linking Client to Care: _____ _____
Phone **Secure Fax**

3) Client was referred to:

Medical Provider/Agency Referred to: _____

Date of referral: _____ **Date of appointment:**_____

Confirmed attendance of appointment (Date verified): _____ **Confirmation method (circle one): Phone or Fax**

Other type of Service Referral: _____

Agency: _____ Date of referral: _____ Date of appointment: _____

Other type of Service Referral: _____

Agency: _____ Date of referral: _____ Date of appointment: _____

Other type of Service Referral: _____

Agency: _____ Date of referral: _____ Date of appointment: _____

Notes/Comments:

ATTACHMENT 18:

Security and Confidentiality Program Requirement Checklist*

1.0 Program Policies and Responsibilities

Standard 1.1

In your program, how are staff members who are authorized to access HIV/VH/STD/TB information or data made aware of their data confidentiality and security responsibilities?

2.1 C. User Responsibilities

Are staff provided training on security policies and procedures and where to find resources?

1.6 Resources & 2.2 B. Security Training

Does the program have written data security and confidentiality policies and procedures?

1.2 Purpose

Are written policies and procedures reviewed at least annually and revised as needed?

2.1 A. Overall Responsible Party

Are data security policies readily accessible to all staff members who have access to confidential, individual-level data?

2.2 A. Verification of Receipt and Assurance of Key Requirements

Where are the policies located?

2.2 A. Verification of Receipt and Assurance of Key Requirements

Standard 1.2

In your program, is there a policy that assigns responsibilities and designates an ORP for the security of the data that is stored in various data systems?

---

*The Centers for Disease Control and Prevention (CDC) National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention (NCHHSTP) *Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs: Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action* Periodic Assessment Checklist

2.1 A. Overall Responsible Party

Does the ORP have sufficient authority to make modifications to policies and procedures and ensure that the standards are met?

2.1 A. Overall Responsible Party

Standard 1.3

Does your program have a policy that defines the roles and access levels for all persons with authorized access?

Table 1: Authorized Access to Confidential Areas/DDP Critical Databases within 6.2 Authorized Data and Database Usage

Does your program have a policy that describes which standard procedures or methods will be used when accessing HIV/VH/STD/TB information or other personally identifiable data?

Figure 1: Network Access Approval Process within 6.2 Authorized Data and Database Usage

Standard 1.4

Does the program have a written policy that describes the methods for ongoing review of technological aspects of security practices to ensure that data remain secure in light of evolving technologies?

2.1 C. User Responsibilities

Standard 1.5

Are written procedures in place to respond to breaches in procedures and breaches in confidentiality?

2.1 C. User Responsibilities & 3.2 E. Incident Handling for Confidentiality Breaches

Where are those procedures stored?

2.1 C. User Responsibilities & 3.2 E. Incident Handling for Confidentiality Breaches

Is the chain of communication and notification of appropriate individuals outlined in the data policy?

2.1 C. User Responsibilities & 3.2 E. Incident Handling for Confidentiality Breaches

Are all breaches of protocol or procedures, regardless of whether personal information was released, investigated immediately to determine causes and implement remedies?

2.1 C. User Responsibilities & 3.2 E. Incident Handling for Confidentiality Breaches

Are all breaches of confidentiality (i.e., a security infraction that results in the release of private information with or without harm to one or more persons) reported immediately to the ORP?

3.2 E. Incident Handling for Confidentiality Breaches

Do procedures include a mechanism for consulting with appropriate legal counsel to determine whether a breach warrants a report to law enforcement agencies?

3.2 E. Incident Handling for Confidentiality Breaches

If warranted, are law enforcement agencies contacted when a breach occurs?

3.2 E. Incident Handling for Confidentiality Breaches

Standard 1.6

Are staff trained on the program's definitions of breaches in procedures and breaches in confidentiality?

3.2 E. Incident Handling for Confidentiality Breaches

Are staff trained on ways to protect keys, use passwords, and codes that would allow access to confidential information or data?

5.9 PC Workstation Accessibility

Are staff trained on policies and procedures that describe how staff can protect program software from computer viruses and computer hardware from damage due to extreme heat or cold?

5.3 Antivirus Software

Have all persons authorized to access individual-level information been trained on the organization's information security policies and procedures?

2.2 B. Security Training

Is every staff member, information technology (IT) staff member, and contractor who may need access to individual-level information or data required to attend security training annually?

2.2 B. Security Training

Is the date of the training or test documented in the employee's personnel file?

2.2 B. Security Training

Standard 1.7

Do all authorized staff members in your program sign a confidentiality agreement annually?

2.2 A. Verification of Receipt and Assurance of Key Requirements

Do all newly hired staff members sign a confidentiality agreement before they are given authorization or access individual-level information and data?

2.2 A. Verification of Receipt and Assurance of Key Requirements

Standard 1.8

Do policies state that staff are personally responsible for protecting their own computer workstation, laptop computer, or other devices associated with confidential public health information or data?

5.9 PC Workstation Accessibility

Are staff trained on ways to protect keys, use passwords, and codes that would allow access to confidential information or data?

5.9 PC Workstation Accessibility

Standard 1.9

Does your program certify annually that all program standards are met?

2.1 A. Overall Responsible Party

2.0 Data Collection & Use

Standard 2.1

When public health data are shared or used, are the intended public health purposes and limits of how the data will be used adequately described?

Attachment 7: Data Recipient Agreement

Standard 2.2

When data are collected or shared, do they contain only the minimum information necessary to achieve the stated public health purpose?

6.5 Data Collection and Use

Standard 2.3

Does your program explore alternatives to using identifiable data before sharing data, such as using anonymized or coded data?

6.3 B. Data Suppression

What alternatives are currently in use in your program?

6.3 B. Data Suppression

Standard 2.4

Does your program have procedures in place to determine whether a proposed use of identifiable public health data constitutes research requiring IRB review?

6.3 A. Research Related Activities

3.0 Data Sharing and Release

Standard 3.1

In your program, is access to HIV/VH/STD/TB information and data for any purposes unrelated to public health (e.g., litigation, discovery, or court order) only granted to the extent required by law?

6.4 Court Ordered Data Access

What non-public health use of the data are required or allowed by law?

6.4 Court Ordered Data Access

Standard 3.2

When a proposed sharing of identifiable data is not covered by existing policies, does your program assess risks and benefits before making decisions to share data?

6.7 C. Non-DDP Programs or Entities

How are these risks assessed?

Attachment 7: Data Recipient Agreement

Standard 3.3

When sharing personally identifiable HIV/VH/STD/TB information and/or data with other public health programs (i.e., those programs outside the primary program responsible for collecting and storing the data), is access to this information and/or data limited to those for whom the ORP:

Has weighed the benefits and risks of allowing access?

6.7 Non-DDP Programs or Entities

Can verify that the level of security established is equivalent to these standards?

6.7 C. Non-DDP Programs or Entities

Standard 3.4

Is access to confidential HIV/VH/STD/TB information and data by personnel outside the HIV/VH/STD/TB programs:

Limited to those authorized based on an expressed and justifiable public health need?

6.7 C. Non-DDP Programs or Entities

Arranged in a manner that does not compromise or impede public health activities?

6.7 C. Non-DDP Programs or Entities

Carefully managed so as to not affect the public perception of confidentiality of the public health data collection activity and approved by the ORP?

6.7 C. Non-DDP Programs or Entities

Before allowing access to any HIV/VH/STD/TB data or information containing names for research or other purposes (e.g., for other than routine prevention program purposes), does your program require that the requestor:

Demonstrate need for the name?

6.3 A. Research Related Activities

Obtain institutional review board (IRB) approval (if it has been determined to be necessary)?

6.3 A. Research Related Activities

Sign a confidentiality agreement?

6.3 A. Research Related Activities

Standard 3.5

Does your program have written procedures to review data releases that are not covered under the standing release policy?

6.7 A. DURSA & Attachment 7: Data Recipient Agreement

If not, does your program have unwritten policy to review data releases that are not covered under the standing release policy?

N/A

Describe briefly those procedures or policies:

N/A

Standard 3.6

Does your program routinely distribute non-identifiable summary data to stakeholders?

6.5 Data Collection and Use

Standard 3.7

Does your program assess data for quality before disseminated?

6.3 B. Data Suppression

Standard 3.8

Does the program have data-release policy that defines access to, and use of, individual-level information?

Attachment 7: Data Recipient Agreement

Does the data-release policy incorporate provisions to protect against public access to raw data or data tables that include small denominator populations that could be indirectly identifying information?

6.3 B. Data Suppression

4.0 Physical Security

Standard 4.1

Are workspaces and paper copies for persons working with confidential, individual-level information located within a secure, locked area?

4.3 Division of Disease Prevention Offices

Are sensitive documents stored in cabinets?

4.4 File Room Access

Are the cabinets locked?

4.4 File Room Access

Are cabinets located in an area to which there is no access by unauthorized employees?

4.4 File Room Access

Are cabinets located in an area to which there is no public access?

4.4 File Room Access

Standard 4.2

Do program staff members shred documents containing confidential information with a cross-cutting shredder before disposing of them?

6.11 Retention/Disposal of Records

Standard 4.3

Does your program have a written policy that outlines procedures for handling paper documents which could contain confidential information that are mailed to, or from, the program?

7.2 Postal/Mailing Services & Attachment 8: Procedure for Mailing Confidential Patient Information

Do staff members in your program ensure that the amount and sensitivity of information contained in any piece of correspondence remains minimal?

7. Data Communications

Standard 4.4

Is access to all secured areas where confidential, individual-level HIV/VH/STD/TB information and data are stored limited to persons who are authorized within policies and procedures (this includes access by cleaning or maintenance staff)?

4.4 File Room Access

Standard 4.5

Do policies include procedures for securing documents containing PII when they cannot be returned to a secure work site by the close of business?

3.2 C. Confidential Data Storage

Do policies outline specific reasons, permissions, and physical security procedures for using, transporting and protecting documents containing PII in a vehicle or personal residence?

3.2 D. Taking PHI into the "field"

If no such procedure exists, is approval obtained from the program manager?

3.2 D. Taking PHI into the "field"

Standard 4.6

When identifying information is taken from secured areas and included in on-line lists or supporting notes, in either electronic or hard-copy format:

> Is it assured that the documents contain only the minimum amount of information necessary for completing a given task?
>
> 7. Data Communications
>
> Is the information encrypted?
>
> 7. Data Communications
>
> Is it coded to disguise information that could be easily associated with individuals?
>
> 7. Data Communications

Do staff members in your program ensure that terms easily associated with HIV/VH/STD/TB do not appear anywhere in the context of data transmissions, including sender and recipient addresses and labels?

7. Data Communications

5.0 Electronic Data Security

Standard 5.1

In your program, are HIV/VH/STD/TB analysis data sets stored securely using protective software (i.e., software that controls the storage, removal, and use of the data)?

6.2 Authorized Data and Database Usage

Are personal identifiers removed from HIV/VH/STD/TB analysis data sets whenever possible?

6.2 Authorized Data and Database Usage

Standard 5.2

In your program, do transfers of HIV/VH/STD/TB data and information and methods for data collection:

Have approval of the ORP?

6.1 Physical Access

Incorporate the use of access controls?

6.1 Physical Access

Encrypt individual-level information and data before electronic transfer?

6.13 A. Data Transferred to CDC

When possible, are databases and files with individual-level data encrypted when not in use?

6.1 Physical Access

Standard 5.3

Does your program have a policy that outlines procedures for handling electronic information and data (including, but not limited to, e-mail and fax transmissions) which may contain confidential information that are sent electronically to or from the program?

7.4 A. Facsimile & 7.4 B. Electronic Mail (E-mail)

When individual-level HIV/VH/STD/TB information or data are electronically transmitted and the transmission does not incorporate the use of an encryption package meeting the encryption

standards of the National Institute of Standards and Technology and approved by the ORP, are the following conditions met?:

The transmission does not contain identifying information.

6.1 Physical Access

Terms easily associated with HIV/VH/STD/TB do not appear anywhere in the context of the transmission, including the sender and recipient address and label.

6.1 Physical Access

Standard 5.4

For all laptop computers and other portable devices (e.g., personal digital assistants [PDAs], other handheld devices, and tablet personal computers [tablet PCs]), which receive or store HIV/VH/STD/TB information or data with personal identifiers, are all the following steps taken to ensure the security of the data?:

The devices have encryption software that meets federal standards.

5.2 Advanced Encryption Standards (AES)

Program information with identifiers is encrypted and stored on an external storage device or on the laptop's removable hard drive.

5.2 A. IronKey™ Flash Drives

External storage devices or hard drives containing the information are separated from the laptop and held securely when not in use.

5.2 A. IronKey™ Flash Drives & 8.4 Electronic Security

The decryption key is kept some place other than on the device.

5.2 Advanced Encryption Standards (AES)

Do the methods employed for sanitizing a storage device ensure that the information cannot be retrieved using "undelete" or other data retrieval software?

5.10 IT-related Surplus, Redistribution, and Disposal

Does the program have policies or procedures to ensure that all removable or external storage devices containing HIV/VH/STD/TB information or data that contain personal identifiers:

Include only the minimum amount of information necessary to accomplish assigned tasks as determined by the program manager

6.1 Physical Access

Are encrypted or stored under lock and key when not in use?

5.2 A. IronKey™ Flash Drives & 6.1 Physical Access

Are sanitized immediately after a given task (excludes devices used for backups)?

6.1 Physical Access

Where are these policies or procedures stored?

6.1 Physical Access

Are hard drives that contain identifying information sanitized or destroyed before the computers are labeled as excess or surplus, reassigned to non-program staff members, or sent off site for repair?

5.10 IT-related Surplus, Redistribution, and Disposal

Standard 5.5

Does your program have policies for handling incoming and outgoing facsimile transmissions to minimize risk of inadvertent disclosure of PII?

7.4 A. Facsimile