

## CONFIDENTIALITY

*Keywords: Confidentiality; protected information; [protected health information](#); [HIPAA](#)*

### Application

This policy applies to all Virginia Department of Health (VDH) personnel whose jobs require handling of confidential information. VDH personnel include classified employees, wage employees, volunteers, assignees (including students), contractors and employees of local government who perform work for VDH. VDH Offices and districts may have additional expectations for confidentiality and are also required to follow this policy and procedures.

### Purpose

Every person has a fundamental right to privacy and confidentiality. This policy defines, identifies and establishes the key components regarding management of confidential information by VDH personnel. This policy covers the handling of all confidential information in an effort to protect confidentiality while balancing VDH's responsibility to protect public health. This policy pertains to all oral, paper based and electronic confidential information. The specific recommended procedures related to management of confidential information are contained in a separate document identified as "Confidentiality Procedures." Procedures are categorized based on the setting in which such information is typically encountered. Finally, in regards to the security and confidentiality of electronic information, VDH abides by the Commonwealth's SEC501 Security Policy in addition to our extended Information Technology Security Manual. Specifics regarding the handling of electronic confidential data are contained in those documents.

### Policy

It is the policy of VDH to protect confidential information. ***Confidential information includes [Protected Health Information \(PHI\)](#) and [Personal Information \(PI\)](#) regarding employees, clients/patients, and the public as well as other forms of confidential information related to proprietary and/or business information.*** This policy requires personnel to take all necessary and proper precautions to appropriately protect confidentiality in their day to day use of confidential information. In a public health setting, confidential information is typically encountered while:

- Providing clinical/patient care services
- Conducting [public health investigations](#)
- Managing human resource records
- Accessing governmental classified information

### Key Components of the Policy

#### 1. Limit Collection of Confidential Information

VDH personnel shall collect confidential information only when such collection is authorized by law or regulation and when confidential information is deemed necessary to further a public health purpose, including when provided to VDH by individuals seeking services. VDH personnel

## CONFIDENTIALITY

shall collect no more confidential information than is reasonably necessary to accomplish their work-related tasks.

### 2. Limit Use of Confidential Information

VDH personnel shall not use confidential information for personal reasons of any kind and shall limit the use of confidential information to only those purposes for which the information was collected or other public health purposes and work-related tasks permitted by law, which furthers the mission of VDH. Whenever identifiable information is not necessary for public health purposes, the confidential information shall be rendered [de-identified](#).

### 3. Limit Access to Confidential Information

VDH personnel shall limit access to confidential information to only those personnel who have a legitimate work-related need to access the information. Access shall be limited to the minimum number of individuals who are reasonably necessary to conduct the work-related purpose.

### 4. Limit Disclosure of Confidential Information

VDH personnel shall limit disclosure of confidential information to only authorized persons. VDH personnel shall follow the confidentiality procedures, which delineate when and to whom disclosures can be made. VDH personnel shall limit disclosure of confidential information to the minimum amount of confidential information necessary to accomplish the intended purpose of the disclosure.

### 5. Acknowledgement of Confidentiality Policy and Procedures

All VDH personnel shall strictly maintain the confidentiality of all confidential information held by the Department. No person having access to confidential information shall disclose, in any manner, any confidential information except as established in the confidentiality procedures. All VDH personnel will receive education and training regarding the confidentiality and security principles addressed in this policy and the procedures. In addition, all VDH personnel shall sign an acknowledgement that they received training and that it is their responsibility to read and comply with all aspects of the Confidentiality Policy and Procedures.

### 6. Data Destruction

As soon as reasonably practicable and in a manner consistent with Commonwealth record retention policies, VDH personnel shall de-identify confidential information and destroy, consistent with processes administered by the Library of Virginia, all identifiable information unless there is a legitimate public health purpose for retaining such identifiable information or retention of the information is required by law. If the confidential data are electronic, please refer to the Commonwealth of Virginia Standard (SEC514: Removal of Commonwealth Data from Electronic Media), VDH Information Security Policy, and applicable HIPAA standards that may apply to the data regarding destruction.

## CONFIDENTIALITY

### 7. Publications and Reports Based on Confidential Information

All reports and publications, internally or externally authored, based on confidential information shall contain only aggregate data. No personally identifiable information or information that could lead to the identification of an individual or facility shall be published or disclosed, unless authorized by the individual or authorized representative or law. All aggregate data presented in such reports or publications shall comply with VDH procedures on aggregate data release to ensure that individuals cannot be identified based on the data presented. No maps based on confidential information may be published or disclosed with sufficient detail so as to allow for identification of individuals.

### 8. Security

VDH personnel who have access to confidential information shall ensure that such information is maintained in a secure manner which prevents unauthorized individuals from gaining access to such information. Confidential information shall not be removed from the work site unless authorized as necessary for work related purposes, shall not be transmitted by email unless by means of a VDH approved secure system (encryption), and shall not be downloaded to a moveable device unless authorized by an office director or equivalent. Moveable devices include desktops and laptops, thumb drives, external hard drives, some printers and copiers, etc. VDH personnel are responsible for securing and protecting moveable devices outside the office environment at all times. Confidential electronic data shall be stored only on a server with appropriate privileges and access parameters. VDH personnel shall follow all applicable procedures to ensure physical and electronic security of all confidential information consistent with the Commonwealth of Virginia Security Policy, Standards, and Guidelines and VDH's Information Security Policy and Standards. VDH personnel shall not attempt to exceed the scope of their authorized access or attempt to or circumvent any VDH systems security measures.

### 9. Data Integrity

VDH will work to ensure the quality, accuracy, and reliability of the data and records under its control, whether contained in written, electronic, or other format. This includes establishing, where appropriate, mechanisms to allow individuals access to review and amend their confidential information if permitted by and in compliance with state and federal law. VDH personnel must ensure that confidential information is protected from unauthorized modification and destruction.

### 10. [Compulsory Legal Process](#), Requests from Law Enforcement and [Freedom of Information Act \(FOIA\)](#) Requests

Any VDH office or district receiving a subpoena, discovery request, FOIA request, court order or any form of compulsory legal process to provide confidential information shall respond pursuant to applicable State and Federal law. The office or district shall seek advice from the Office of the Commissioner (OCOM) and/or the Office of the Attorney General (OAG) as determined by the respective Deputy Commissioner. Guidance for VDH employees responding to requests for

## CONFIDENTIALITY

access to patient medical records and subpoenas is posted on the FOIA page of the VDH internal website

### 11. Non-Compliance

All VDH personnel are required to comply with the Confidentiality Policy as well as Privacy/Security Standards, Policies and procedures referenced. VDH personnel that fail to comply may be denied further access to confidential information and may be subject to disciplinary action up to and including termination. VDH personnel shall immediately report to their supervisor any violations of this policy. VDH may audit use and disclosure of confidential information by VDH personnel to ensure compliance with this policy and the procedures. **The Confidentiality Policy and Procedures continue to apply to personnel after leaving VDH, with respect to confidential information to which the individual had access while working at VDH.**

#### Authority

Each specific authority is cited in the relevant section of the confidentiality procedures.

#### Related Policies

Each related policy is cited in the relevant section of the confidentiality procedures.

#### Glossary

##### 1. Compulsory legal process

A term that encompasses not only a subpoena, which is a command to appear at a particular time and location to provide testimony or records upon a certain matter, but also a search warrant and a bench warrant, which is a written order commanding a law enforcement officer to seize the person named and bring that person into court.

##### 2. De-identified data

Under the [Health Insurance Portability and Accountability Act of 1996 \(HIPAA\)](#) Privacy Rule, data are de-identified if either (1) an experienced expert determines that the risk that certain information could be used to identify an individual is "very small" and documents and justifies the determination, or (2) the data do not include any of the following eighteen identifiers (of the individual or his/her relatives, household members, or employers) which could be used alone or in combination with other information to identify the subject: names, geographic subdivisions smaller than a state (including city/county (unless the locality contains greater than 20,000 residents) or zip code except that the first three digits of zip code may be used if the area contains > 20,000), all elements of dates except year (and even year of birth cannot be used if the subject is greater than 89 years old), telephone numbers, FAX numbers, email address, Social Security numbers, medical record numbers, health plan beneficiary numbers, account

## CONFIDENTIALITY

numbers, certificate/license numbers, vehicle identifiers including license plates, device identifiers and serial numbers, URLs, internet protocol addresses, biometric identifiers, full face photos and comparable images, and any unique identifying number, characteristic or code; note that even if these identifiers are removed (= redacted – See Code of Virginia [§32.1-127.1:05](#)), the Privacy Rule states that information will be considered identifiable if the covered entity knows that the identity of the person may still be determined.

### 3. Family Educational Rights and Privacy Act (FERPA)

FERPA, 20 U.S.C. § 1232g and 34 CFR Part 99 (amended 12/08) is a federal law that protects the privacy of student education records. Records covered by FERPA are exempt from the [HIPAA](#) Privacy Rule. Generally, schools must have written parent (or eligible student) permission to release any information from a student’s education records. However, FERPA allows disclosure of personally identifiable records, without consent, under certain conditions. These include disclosure to appropriate officials if the information is necessary to protect the health or safety of the student or other individuals ([34 CFR § 99.36](#)).

### 4. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA was 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 ([42 C.F.R. Part 3 \(73 FR 70732\)](#)) 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,” including surveillance. ([45 CFR 164.512\(b\)](#)) The HIPAA regulations exclude information considered “education records” under [FERPA](#) from HIPAA privacy requirements.

### 5. Medico-legal

Medico-legal refers to aspects of the law that relate to the practice of medicine or health. It includes forensic medicine where medical investigation results in the provision of evidence to the legal process.

### 6. 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

## CONFIDENTIALITY

institution. PI includes information such as race, sex, age, home address, home telephone number, marital status, dependents' names, insurance coverage, or Social Security Number. "Personal information" shall not include routine information maintained for the purpose of internal office administration whose use could not be such as to affect adversely any data subject nor does the term include real estate assessment information. There is "personal information" that is routinely used in agency emails that is not subject to this policy and every staff member should use discretion and professional knowledge to make that determination. If you remain uncertain as to whether or not this policy applies to the personal information you are using, seek guidance from your management.

Commonwealth Security Standards (SEC501-09) further defines personal information as it relates to the classification of IT Systems as:

*"Personal information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:*

- 1. Social security number;*
- 2. Driver's license number or state identification card number issued in lieu of a driver's license number; or*
- 3. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts.*

*The term does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.*

### **7. Personnel**

This includes classified employees, wage employees, volunteers, assignees (including students), contractors and employees of local government who perform work for VDH.

### **8. Protected 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).

### **9. Public Health Investigations**

For the purposes of this policy, public health investigations include the core public health activities of surveillance and investigation as well as VDH health oversight activities such as surveys, inspections, contacting clients or providers as necessary for public health program

## CONFIDENTIALITY

activities, as well as [medico-legal](#) death or other investigations, management of registries or collection and management of any other data sets related to a mandated or contracted public health activity.

### 10. Public Record

A public record is any writing or recording -- regardless of whether it is a paper record, an electronic file, an audio or video recording, or any other format -- that is prepared or owned by, or in the possession of a public body or its officers, employees or agents in the transaction of public business. All public records are presumed to be open, and may be withheld only if a specific, statutory exemption applies.

### 11. Virginia Freedom of Information Act (FOIA)

FOIA is a state law, located § [2.2-3700](#) et. seq. of the Code of Virginia, which guarantees citizens of the Commonwealth and representatives of the media access to [public records](#) held by public bodies, public officials, and public employees. The purpose of FOIA is to promote an increased awareness by all persons of governmental activities. The FOIA statute is to be interpreted liberally, in favor of access, and any exemption allowing public records to be withheld must be interpreted narrowly.

### Frequently Asked Questions

Please go to the Confidentiality Policy web page for these.

### Training

Training is available and required on the handling and use of confidential records during new employee orientation, through the required on-line TRAIN Course #1032033, "Protecting Confidential Information at VDH", **and** on-the-job training by supervisor. Employees routinely handling said information must renew their knowledge of the policy every other year in keeping with the review cycle. Supervisors are responsible to see that the training is completed.

### Policy Administration

This policy will be reviewed and updated by VDH senior leadership no less frequently than once every two years.

## CONFIDENTIALITY

### Index

- Confidentiality Procedures
- I. General Provisions
- II. Protection of Confidential Information Obtained during Direct Patient Care Provision
- III. Protection of Confidential Information Collected during the Course of a Public Health Investigation Outside a Direct Clinical Care Context
- IV. Protection of Human Resources Workforce Confidential Information
- V. Protection of Federally Classified Information
- VI. Resources

## CONFIDENTIALITY

### Confidentiality Procedures

The following Confidentiality Procedures sections provide summary and detailed information about managing confidential information at VDH. Although not meant to provide a step by step approach to information management, they do provide summary and detailed information generally applicable to all VDH personnel and then more specifically relevant to particular roles within VDH. Each section will clarify who is required to review the section in detail. All of the information is available to all VDH personnel as a resource and will form the basis of ongoing training within the agency.

#### Table of Contents for Confidentiality Procedures

- I. [General Provisions](#)
- II. [Protection of Confidential Information Obtained during Direct Patient Care Provision](#)
- III. [Protection of Confidential Information Collected during the Course of a Public Health Investigation Outside a Direct Clinical Care Context](#)
- IV. [Protection of Human Resources Workforce Confidential Information](#)
- V. [Protection of Federally Classified Information](#)
- VI. [Resources](#)
- VII. [Blank Employee General Confidentiality Agreement](#)

## CONFIDENTIALITY

### I. General Provisions

The provisions of this section are more general in nature and apply to many of the core services provided within VDH. **All VDH personnel must review this section of the Confidentiality Procedures.**

#### 1) Introduction

It is expected that Virginia Department of Health (VDH) staff will come into contact with confidential information (i.e., [protected health information \(PHI\)](#) or [personal information \(PI\)](#)) of one sort or another during the course of their workday. Confidential information includes that which either directly identifies an individual or contains elements that could potentially be used alone or in combination to identify an individual. Data elements that are directly or potentially identifiable, and for which confidentiality must be maintained, have been defined in the de-identification standard of the [HIPAA](#) Privacy Rule (45 CFR 164.514). These elements include the following:

- a) Name
- b) Address (all geographic subdivisions smaller than state, including street address, city, county, zip code, except that the first three digits of zip code may be used if the area contains > 20,000 people)
- c) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- d) Telephone numbers
- e) Fax number
- f) Email address
- g) Social Security number
- h) Medical record number
- i) Health plan beneficiary number
- j) Account number
- k) Certificate/license number
- l) Any vehicle or other device serial number
- m) Device identifiers or serial numbers
- n) Web URL
- o) Internet Protocol (IP) address numbers
- p) Finger or voice prints
- q) Photographic images
- r) Any other characteristic that could uniquely identify the individual

VDH staff may encounter confidential information while:

## CONFIDENTIALITY

1. Providing clinical/patient care services
2. Conducting [public health investigations](#)
3. Managing human resource records
4. Accessing governmental classified information

All individuals working at or on behalf of VDH who come into contact with [protected health information \(PHI\)](#) must maintain the confidentiality of an individual's health information at all times. Protections for the privacy of individually identifiable health information are contained within the [Health Insurance Portability and Accountability Act of 1996 \(HIPAA\)](#). The major goal of HIPAA is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote quality care. The key elements of HIPAA include the use and disclosure of PHI, authorization for any use and disclosure, adherence to the principle of "minimum necessary" use and disclosure, and privacy practices notice.

VDH personnel responsible for the provision of clinical or patient care services will encounter PI or PHI during their interactions with clients. Privacy protections are intended to provide VDH clients with assurance that their health information will be properly protected while not compromising either the availability or the quality of medical care. **All VDH personnel who are involved in clinical or patient care services must review Confidentiality Procedures Section II.**

Those individuals conducting [public health investigations](#) will encounter PHI and other confidential information such as names of affected businesses or other organizations for example. These investigations are governed both by agency policy and law and require the investigator to be educated about the limits of their actions as well as those of the State Health Commissioner and the agency as a whole. **All VDH personnel who are involved in [public health investigations](#) must review Confidentiality Procedures Section III.**

For managers and others handling human resource records, agency and the Department of Human Resource Management (DHRM) policy, best practices and state and federal law dictate the handling of that information. VDH provides the necessary training to individuals to assure appropriate handling of these records. **All VDH personnel who are involved in handling human resources records must review Confidentiality Procedures Section IV.**

In its emergency preparedness role, key VDH personnel are integrated into the Commonwealth's homeland security actions and, as such, have been cleared to handle federally classified materials. However, there are strict guidelines that include space and equipment requirements as outlined in **Section V. Administrative Procedures for the Protection of Federally Classified Information**. The Secretary of Veterans Affairs and Homeland Security for the Commonwealth provides training for those with clearances. Equally important, however, is that those without such clearances be fully informed of their limitations interacting with federally classified information to avoid security breaches. **All VDH personnel with federal clearances must review Confidentiality Procedures Section V.**

## CONFIDENTIALITY

VDH provides the information technology (IT) applications necessary to manage this information. The Virginia Information Technologies Agency/Northrop Grumman partnership provides the infrastructure on which the applications reside and is therefore responsible for network security in addition to all VDH employees who access that network. All employees are expected to follow agency policy and Commonwealth standards for the management of this information technology (as outlined in the Commonwealth Policy, Standards and Guidelines, specifically, the Commonwealth Security Standard (SEC501)) and the VDH Information Security Policy and Standards.

Any VDH personnel who might have access to confidential information in the course of conducting their work duties must receive training on the VDH Confidentiality Policy and the overall importance of protecting confidentiality. VDH personnel will be required to sign a statement assuring that all necessary measures will be taken to protect confidentiality, prior to initiation of related activities.

### 2) Common Procedures

Certain procedures apply to all VDH personnel. These include protection of confidential information in VDH workspaces and the [Freedom of Information Act](#).

#### a) *Protection of Confidential Information in VDH Workspaces*

- i) Confidential records must be kept locked up at all times when they are not actually being used. That is, they must be kept in locked cabinets or in locked rooms or offices after business hours and whenever the persons using them are not present.
- ii) If records are maintained in electronic form, the medium on which the files are stored (e.g., CD's, thumb drives/flash drives, and removable hard drives) must also be kept in locked containers or, if maintained on a computer, access secured by all reasonable available means (including keyboard locks, passwords, encryption) and office locks.
- iii) Computers, desktop or laptop, containing confidential records should never be maintained in an open, unsecured space. Only a limited number of authorized staff may have keys or other means of access to cabinets or rooms where equipment containing confidential information is stored. As previously stated, confidential information shall not be removed from the work site unless authorized as necessary for work related purposes, shall not be transmitted by email unless by means of a VDH approved secure system (encryption), and shall not be downloaded to a moveable device unless authorized by an office director or equivalent. Moveable devices include desktops and laptops, thumb drives, external hard drives, some printers and copiers, etc.
- iv) When confidential records are in use, whether by themselves or viewed on computer monitors, they must be kept out of the sight of persons not authorized to work with the records.
- v) Fax machines that are used to receive and/or transmit confidential information must be located in an area where documents can be screened from the casual viewer. This area should be locked after hours or when not attended by authorized individuals.

## CONFIDENTIALITY

- vi) Except as needed for operational purposes, copies of confidential records (i.e., paper documents, electronic files, video recordings, or records of other kinds) are not to be made. Any duplicate copies made of confidential records are to be destroyed as soon as operational requirements permit. Approved means of destruction include shredding, burning, and macerating. Approved means of destruction for electronic data are described in the Commonwealth of Virginia Standard (SEC514: Removal of Commonwealth Data from Electronic Media), VDH Information Security Policy, and applicable HIPAA standards .
  - vii) Reuse of electronic media (e.g., hard drives and rewriteable compact disks) containing confidential records should be accomplished in a manner consistent with the Commonwealth of Virginia Standard (SEC514: Removal of Commonwealth Data from Electronic Media).
  - viii) Disposal of electronic media (e.g., hard drives and rewritable compact disks) containing confidential records should be performed in a manner consistent with procedures outlined in the Commonwealth of Virginia Standard (SEC514: Removal of Commonwealth Data from Electronic Media), VDH Information Security Policy, and applicable HIPAA standards..
  - ix) No record containing direct personal identifiers (e.g., name, address, social security or other identifying number, unretouched video, or audio recording) may be electronically sent to or accessed from a home or telecommuting work site or removed from offices except as required in the conduct of data collection activities. No confidential information may reside on a personal or home use computer at any time, unless the staff member provides his/her own cell phone per the Bring Your Own Device Policy.
  - x) **Records that contain identifying information must be destroyed within six months of the expiration of the records retention period (Code of Virginia § [42.1-86.1](#)).**
- b) *Sharing of confidential information within VDH*
- i) At times it is necessary to share confidential information with coworkers and supervisors as part of public health operations. Discussions of confidential information should be kept to a minimum and include only those with a public health need to know. Such discussions should only be held in private areas, preferably behind closed doors, and never in hallways, elevators or other open areas.
  - ii) Use of email to communicate confidential information should be done in accordance with VDH Information Security Policy and the Commonwealth Security Policy, Standards and Guidelines. Users may be subject to additional requirements depending on the nature and subject of the confidential information to be transmitted. The following requirements shall be considered as minimum expectations for sensitive or confidential information:
    - (1) VDH requires that all data that are considered sensitive relative to confidentiality or integrity be encrypted during transmission (Commonwealth Security Standard SEC501). Information defined as sensitive under HIPAA HITECH Act may require additional safeguards for compliance.

## CONFIDENTIALITY

- (2) Email shall not be used to send sensitive data unless encryption complying with the Commonwealth Security Standard is used. In general, this shall also meet the National Institute of Standards and Technology requirements under NIST SP800-45 and SP800-52.
  - (3) Microsoft Office (2007 and later) products may meet the security requirement if the Microsoft encryption option with a strong credential / password is used. The document password will need to be shared with the document recipient in a secure manner (i.e., in a separate communication).
  - (4) Names of individuals whose confidentiality must be protected, such as those who are receiving care from or being investigated by public health, shall not be included in the text of any email; however, use of initials is acceptable.
  - iii) Steps must be taken to ensure the security of confidential information that is transmitted or received by fax. This would include a cover sheet clearly identifying the recipient or addressee and their contact information along with a confidential information statement outlining steps required to be taken if the information is received by an unauthorized individual.
  - iv) Data that are shared between programs should be protected according to the rules and procedures of the program that initially hosted the data. It is preferable for data sharing arrangements to be defined in a signed agreement. No data should be released without the appropriate managerial approvals.
  - v) No individual identifiers shall be included in any data report.
- c) [Virginia Freedom of Information Act \(FOIA\)](#)
- VDH, as part of the Executive Branch of government, must also act in a manner consistent with other governmental entities. Governmental transparency requires that information is released when it should be and, even more importantly, that information not be released when it is protected from such requests. All VDH personnel must be aware of those aspects of the Virginia FOIA that impact their work. Generally, with respect to FOIA requests, the following conditions apply:
- i) VDH often receives FOIA requests for which several different work units within the agency (e.g., Central Office, Districts, Departments) may have documents that are responsive to the request.
  - ii) Regardless of whether such a request is received at the local, district, regional or central office level, personnel efforts related to searching for, reviewing and producing responsive documents should be coordinated with all other levels of the agency so that only a single, coordinated agency response is submitted.
  - iii) VDH personnel receiving a request for information should refer to the agency's FOIA guidance ([http://vdhweb/Admin/FOIA\\_Guidance.asp](http://vdhweb/Admin/FOIA_Guidance.asp)) for more detail. VDH staff should direct any questions to the Agency FOIA coordinator. Response to certain questions may require advice from the Office of the Attorney General (OAG).
  - iv) The identities and identifying information of patients and providers must be removed before submission of information to the requestor unless the request comes from the

## CONFIDENTIALITY

patient or provider and the response contains only information pertaining to that individual or the request includes a signed authorization from the individual.

- v) Select agent (those determined to have the potential to pose severe threat to human health) information may not be released in response to a FOIA request (Code of Virginia § 32.1-36.F.2 and § 2.2-3700 et seq.).

Other health information is also exempted from Virginia's FOIA statute. A list of health exemptions is contained in § [2.2-3705.5](#) of the Code of Virginia. Refer to the agency's FOIA guidance for additional exemptions that are applicable to records and information maintained by VDH.

## CONFIDENTIALITY

### II. Administrative Procedures for the Protection of Confidential Information Obtained during Direct Patient Care Provision

The provisions of this section apply to any VDH personnel who are involved in any aspect of direct patient care provision. **All VDH personnel involved in any aspect of direct patient care provision must review this section of the Confidentiality Procedures. Other VDH personnel should refer to this section as a resource when needed.**

#### Summary of Use

- Do not use or disclose [protected health information](#) unless specifically required or permitted by law or unless authorized in writing by the individual who is the subject of the information.
- A health care provider that has a direct treatment relationship with an individual is not required by the [HIPAA](#) Privacy Rule or Virginia's Patient Health Records Privacy Act to obtain an individual's authorization prior to using and disclosing information about him or her for treatment, payment and health care operations.
- VDH is permitted to use and disclose [protected health information](#) without an individual's authorization in the following most common situations: (1) to the individual, (2) for treatment, payment and health care operations, (3) to someone other than the client as in the case of child and adult abuse investigation requirements, (4) for public health activities such as disease reporting, (5) for workmen's compensation cases as permitted, (6) in response to a court order or a subpoena or (7) other disclosures as permitted by law.
- When authorization is required it must contain specific information regarding the information to be disclosed or used, the person disclosing and receiving the information, the date the authorization expires, and the right to revoke the authorization.
- Each individual seen for medical care must be provided with a Notice of Privacy Practices. Each individual must acknowledge in writing receipt of the privacy practices notice. This statement is contained on the CHS 1-A, Patient Application and Consent for Health Care.
- VDH has developed [HIPAA](#) policies and procedures which are all posted on the HIPAA web site (<http://vdhweb/hipaa/>).
- Questions about specific situations or breach of privacy must be communicated promptly through the supervisory chain.

#### 1) Introduction

## CONFIDENTIALITY

Agency protections for the privacy of individually identifiable health information are contained within the document titled [Virginia Department of Health Release of Protected Health Information](#), (updated September, 2011). It is VDH policy to require all covered functions, Business Associates, and individuals that come into contact with [protected health information \(PHI\)](#) to maintain the confidentiality of an individual's identified health information at all times. Privacy protections are intended to provide VDH clients with assurance that their health information will be properly protected while not compromising either the availability or the quality of medical care.

In accordance with provisions set forth by the U.S. Department of Health and Human Services (HHS), [Health Insurance Portability and Accountability Act of 1996 \(HIPAA\)](#), HHS issued *The HIPAA Privacy Rule*, December, 2000 and amended it as recently as 2013. HHS defines PHI as information that relates to the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, the past present or future payment of the provision of health care to the individual along with demographic data for which, "there is a reasonable basis to believe can be used to identify the individual." Per 45 CFR, § 164.501 PHI is "individually identifiable health information (with limited exceptions) in any form, including information transmitted orally, or in written or electronic form. "

The key elements contained within the Privacy Rule are as follows:

- a) Authorization
- b) Parents as the personal representative of unemancipated minors
- c) Uses and disclosures for treatment, payment, and health care operations
- d) Uses and disclosures for which authorization is required
- e) Minimum necessary uses and disclosures, and oral communications
- f) Uses and disclosures for marketing
- g) Uses and disclosures for research purposes
- h) Notice of Privacy Practices
- i) De-identification
- j) Business associates
- k) Breach Notifications

### 2) **Summary of the Provisions of the [HIPAA Privacy Rule](#)**

VDH may not use or disclose [protected health information](#), except either as the Privacy Rule permits or requires or as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing (refer to Department of Health and Human Services, Office for Civil Rights [OCR] *Privacy Rule Summary*, revised May 2003).

Written authorization must be obtained from individuals to use and disclose their [protected health information](#). However, a health care provider that has a direct treatment relationship with an individual is not required by the Privacy Rule to obtain an individual's authorization before using and disclosing information about him or her for treatment, payment and health care operations.

## CONFIDENTIALITY

VDH is permitted to use and disclose [protected health information](#) without an individual's authorization in the following situations: (1) to the individual, (2) for treatment, payment and health care operations, (3) to someone other than the client as in the case of child and adult abuse investigation requirements, (4) for public health activities such as disease reporting and [public health investigations](#), (5) for worker's compensation cases, (6) in response to a court order or a subpoena (7) other disclosures as required by law. In most other situations, VDH must obtain an individual's written authorization to use and disclose PHI. The authorization must contain specific information regarding the information to be disclosed or used, the person disclosing and receiving the information, the date the authorization expires, and the right to revoke the authorization. Except for treatment purposes, VDH must make reasonable efforts to use, and disclose only the minimum amount of [protected health information](#) needed to accomplish the intended purpose of the use, disclosure or request (i.e., Minimum Necessary Guidance).

In addition, each individual seen for medical care must be provided with a Notice of Privacy Practices. The notice describes the ways in which VDH may use and disclose PHI. The notice states VDH's duties to protect privacy, the individual's right, and a point of contact for making a complaint. Each individual must acknowledge in writing receipt of the privacy practices notice. This statement is contained on the CHS 1-A, Patient Application and Consent for Health Care.

[HIPAA](#) forms that must be given to every client seen in the clinic, home, or office are described in full in the document titled *Office of Privacy and Security, Use and Filing of HIPAA Forms*. Links to the following appear on the HIPAA web page (<http://vdhweb/hipaa/>).

- a) Use and Filing of HIPAA Forms
- b) Notice of Privacy Practices
- c) Authorization for Disclosure of [Protected Health Information](#)
- d) Authorization for Disclosure of Protected Health Information Implementation Specifications and Directives
- e) Request to Rescind Authorization
- f) Complaint Form for Complaint to District Office
- g) District Complaint Log
- h) Complaint Form for Complaint to Agency Office of Privacy and Security
- i) Agency Complaint Log
- j) Request for Inspection of [Protected Health Information](#)
- k) Right to Request an Amendment
- l) Medical Record Amendment/Correction Form
- m) Acknowledgement of Amendment
- n) Disclosure of Medical Information and Disclosure Log
- o) Request for Accounting of Disclosures of Protected Health Information

Personnel and administrative policies and procedures such as workforce training and management, confidentiality agreement, a HIPAA Employee Sanction policy, a HIPAA Governance Policy, Medical



Office of the Commissioner  
VDH Policy Number: OCOM #1.01  
Effective Date: 05/9/2012  
Last Revision Date: 07/10/2015  
Review Cycle: 08/01/2017  
Reviewer: Deputy Commissioner for Administration

## **CONFIDENTIALITY**

Records Management, and a Business Associate Agreement template have been developed to ensure compliance with the Rule. Each of these policies and procedures is posted on the HIPAA web site (<http://vdhweb/hipaa/>).

To minimize the likelihood of a HIPAA breach, compliance with the Privacy Rule is essential. HHS may impose sanctions to include monetary penalties for failure to comply with a Privacy Rule requirement.

## CONFIDENTIALITY

### III. Administrative Procedures for the Protection of Confidential Information Collected during the Course of a Public Health Investigation Outside Direct Clinical Care Context

The provisions of this section apply to any VDH personnel who are involved in any aspect of [public health investigations](#) apart from the provision of direct patient care. **All VDH Personnel involved in any aspect of public health investigation must review this section of the Confidentiality Procedures.**

#### Summary of Use

Protection of information while working in the field:

- VDH personnel using confidential information in the field are responsible for the security of those data and should only possess data with the knowledge and approval of their supervisor.
- Confidential information taken into the field, or collected in the field, as part of an investigation should never be left unattended and should be stored securely. No confidential information should be visible to others.
- Electronic records containing confidential information should be encrypted before they are taken outside the office.
- VDH staff should ensure that the purpose of their presence in the field while conducting a confidential investigation is not apparent to the casual observer.
- No record containing direct personal identifiers may be electronically sent to or accessed from a home or telecommuting work site or removed from offices except as required in the conduct of data collection activities.

Sharing of confidential information within VDH:

- Discussions of confidential information should be kept to a minimum and include only those with a public health need to know and be held in private settings.
- Use of email to communicate confidential information should be done in accordance with the Office of Information Management's (OIM) *Information Technology Resources Management Policy and Procedures*, as follows:
  - VDH requires that all data that are considered sensitive relative to confidentiality or integrity be encrypted during transmission; and
  - Names of individuals being investigated by public health should not be included in the text of any email; however, use of initials is acceptable.
- No VDH personnel shall release any data that were collected unless permission from the responsible office director or equivalent has been obtained.
- No individual identifiers shall be included in any data report.

## CONFIDENTIALITY

Sharing of confidential information outside VDH with the following:

The individual:

- Confidential information about an individual may be communicated to that individual, the legal designee for that individual, or to a parent or guardian if the individual is a minor, within the limitations of State and Federal regulations.
- Consent forms should be signed by the individual, or the legal designee for that individual, before the collection of a specimen that requires an invasive procedure.
- Disclosure of confidential information to contacts of an individual should rarely be necessary and should be avoided to the highest extent possible except as allowed by the Code of Virginia. Such disclosure may occur only if authorized by the State Health Commissioner.

Healthcare providers and facilities:

- Confidential medical information collected by VDH during the course of an investigation may be shared with the medical care provider of the individual, with the patient's, or legal designee's, authorization.

Businesses and other non-healthcare settings:

- Confidential information about an individual in these settings should not be shared with anyone in the setting other than the individual. To do otherwise would require authorization by the Commissioner.
- It is the policy of VDH not to, on its own initiative, release the names of businesses under investigation to the public unless the business fails to comply with public health recommendations and continues to pose a risk to the public's health. Prior to such a release, VDH personnel must have the concurrence of the Office of the Commissioner (OCOM) and the business should be notified of VDH's intent to share the information. Additionally, as a state agency, VDH is subject to the [Freedom of Information Act \(FOIA\)](#) and if faced with a FOIA request for the identity of a business, VDH will need to comply unless an applicable FOIA exclusion exists.

Other Governmental Agencies:

- VDH staff must extend the confidentiality policy to these interactions and disclose information only when it is necessary for the investigation. There are exceptions noted in the confidentiality procedures.

## CONFIDENTIALITY

Court orders and subpoenas:

- Court orders may require the release of certain confidential information; before releasing the requested information, the office or district shall seek advice from the OCOM and/or the Office of the Attorney General (OAG) as determined by the respective Deputy Commissioner.

Media:

- VDH staff shall never release the name or identifying information of any patient or provider to the media unless approved by the Commissioner. Specific guidance is contained in the confidentiality procedures.

### 1) Purpose

VDH has a legal and ethical obligation to protect the confidentiality of records collected in the course of public health work conducted outside of providing direct clinical care, such as in the course of conducting surveillance, inspections, and investigations. This document establishes a framework for every VDH program/district to follow in order to ensure that consistent rules are applied and appropriate procedures are followed in a manner that protects the identities of our residents, affected establishments, and those who report information to VDH, as required by law. VDH programs/districts may have policy and procedures which are more restrictive than what is contained herein.

### 2) Legal mandates to protect confidentiality

Confidentiality means keeping protected information to oneself and sharing only as allowed by law and policy and only as essential for conducting public health activities. Section VI **Resources** contains relevant sections of federal and state laws and regulations governing confidentiality for VDH programs. In addition, policy and professional ethical standards can provide protection of information beyond that which is legally mandated.

At times, requirements to protect information go beyond confidentiality. For example, according to the Code of Virginia, the identity of “each patient and practitioner of the healing arts whose records are examined pursuant to §32.1-40” must be anonymous. These are records examined as part of ‘investigation, research or studies of diseases or deaths of public health importance’. Anonymous means that there is no way anyone else can know the identity of these patients and providers. The State Health Commissioner is the only one who is legally authorized to ever divulge this type of information, can do so only if pertinent to an investigation, research or study, and the person to whom the information is divulged must preserve the anonymity of the information ([§32.1-41](#)).

## CONFIDENTIALITY

### 3) Procedures for Storing Confidential Information

- a) When unattended, confidential information shall be stored in a locked filing cabinet, locked desk drawer, a locked overhead storage compartment such as systems furniture credenza, or a similar locked compartment.
- b) Information can also be stored in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without the need-to-know, such as a locked room or an area where access is controlled by a guard, cipher lock, or card reader.

### 4) Activities that require adherence to confidentiality policies

Many daily VDH public health activities require the handling of confidential information. VDH employees are expected to use all available reasonable means to protect confidentiality in all these settings and forms of communication. In this document, the areas of activity will be grouped into the following categories, each of which will be discussed in more detail below:

- a) Protection of information including moveable media at all times while working in the field
- b) Sharing of confidential information outside VDH, specifically with the following entities:
  - i) The individual
  - ii) Healthcare providers and facilities
  - iii) Businesses and other non-healthcare settings
  - iv) Other governmental agencies
  - v) Media
- c) FOIA
- d) Court orders and subpoenas
- e) Statistical reports
- f) Non-routine data requests

### 5) Procedures for Protection of Information While Working in the Field

- a) VDH staff using confidential information in the field are responsible for the security of those data and should only possess confidential data with the knowledge and approval of their supervisor.
- b) Confidential information taken into the field, or collected in the field, as part of an investigation should never be left unattended and should be stored securely. No confidential information should be visible to others.
- c) Electronic records containing confidential information should be encrypted before they are taken outside the office.
- d) VDH staff should ensure that the purpose of their presence in the field while conducting a confidential investigation is not apparent to the casual observer.
- e) Moveable devices including laptops shall be secured in a non-visible location (i.e., locked trunk) during travel and removed from the vehicle at night.
- f) Photographs taken in the course of conducting public health investigations that could potentially identify an individual whose confidentiality needs to be protected, including pictures of faces or homes, should be treated as confidential in the same way confidential documents

## CONFIDENTIALITY

are treated. Photographs should be taken and/or shared only if the picture is necessary to convey important public health information. The identity of any individual in a photograph should be protected by placing a black bar over the eyes or applying some other means of disguising identifying features. Permissions should be granted by the photographed person, or the parent of a minor, prior to taking the picture.

### 6) Procedures for Sharing Confidential Information outside VDH

- a) The individual
  - i) Confidential information about an individual may be communicated to that individual, the legal designee for that individual, or to a parent or guardian, if the individual is a minor, within the limitations of State and Federal law, or to a legal representative or next of kin if the person is not competent to understand the information being communicated.
  - ii) Persons have the right to examine information collected about them by the health department.
  - iii) Information may be released to attorneys if the request is accompanied by an authorization signed by the individual or a legal representative of the individual. Additional information related to court orders is addressed elsewhere in this document.
  - iv) If an individual is deceased, health records may be released consistent with Virginia law (Va. Code § 32.1-127.1:03(D)(24)) which provides that “[h]ealth care entities may, and when required by other provisions of state law, shall disclose health records . . . (i) If the health records are those of a deceased or mentally incapacitated individual to the personal representative or executor of the deceased individual or the legal guardian or committee of the incompetent or incapacitated individual or if there is no personal representative, executor, legal guardian or committee appointed, to the following persons in the following order of priority: a spouse, an adult son or daughter, either parent, an adult brother or sister, or any other relative of the deceased individual in order of blood relationship.”
  - v) Consent forms should be signed by the individual, or the legal designee for that individual, before the collection of a specimen that requires an invasive procedure. If the individual is a resident in a group facility without a Medical Director, it may be appropriate to have the individual identify additional persons who may receive test results at the time that they sign the consent form and to note that on the form to facilitate timely public health action.
  - vi) Disclosure of confidential information to contacts of an individual should rarely be necessary and should be avoided to the highest extent possible except as allowed by law. Every effort should be made to convey the information needed for control measures to be implemented or other public health actions to be taken without naming the ill individual. In the event that approach is unsuccessful, VDH should ask the person or his/her legal representative to make the disclosure themselves to prevent disclosure by public health staff, and upon refusal, explain the necessity and rationale for the disclosure and seek written authorization from the patient or their legal representative permitting the health department to disclose the necessary information. In the rare event that these steps fail and disclosure of confidential information to contacts of an individual is considered necessary for the particular public health investigation, such disclosure may occur only if authorized by the Commissioner.

## CONFIDENTIALITY

- b) Healthcare providers and facilities
  - i) Confidential medical information collected by VDH during the course of an investigation may be shared with the medical care provider of the individual, with the patient's or legal designee's authorization. The medical care provider is defined as the attending physician directly providing care for the individual and/or the submitter of a sample for laboratory testing.
  - ii) In the instance that the individual is a resident in a group facility with a Medical Director, the Medical Director or his or her designee (i.e., Director of Nursing, Infection Preventionist) may receive test results from specimens collected by VDH, in order to facilitate timely public health action.
  - iii) In the instance that the individual is a resident of a group facility that does not have a Medical Director, the Director of Nursing for the facility may receive test results from specimens collected by VDH if the public health investigators have determined that the person in that position needs that level of confidential information in order to protect the health of current or future residents.
  - iv) Administrators of group facilities are not considered medical care providers and should not receive confidential medical information on a resident of the facility without the resident's authorization or that of a legal representative of the resident, unless this is required as part of a facility regulatory survey, for example as outlined in the General Procedures in the Centers for Medicare and Medicaid Services State Operations Manual.
  - v) Results of testing conducted on staff of a facility shall not be shared with any other representative or staff of the facility, including the medical director or director of nursing, unless the person who was tested agrees to such disclosure in writing. If the staff member continues to pose a threat to public health, then the provisions in the following section apply.
- c) Businesses and other non-healthcare settings
  - i) Examples of businesses potentially interested in confidential information collected in [public health investigations](#) may include day care centers, restaurants, hotels, and workplaces.
  - ii) Confidential information about an individual in these settings should not be shared with anyone in the setting other than the individual. At times, public health actions must be taken in these settings in order to contain the public health threat. When that is the case, every effort should be made to institute the necessary control measures without identifying any ill individual. If the identity of an individual becomes known in the setting, those who are aware of the identity should be reminded of the importance of protecting the confidentiality of that information and how information can be communicated to others without violating confidentiality. The ill individual(s) should be encouraged to share information with the facility/business director if that would aid the implementation of public health actions. If he/she is unwilling to do so and the public health investigator believes such disclosure is necessary for successful accomplishment of the public health mission, the investigator should inform the individual that the investigator will have to notify the

## CONFIDENTIALITY

- business if the individual refuses to do so and that such action is necessary to protect the health of others in that setting. The investigator should seek written authorization to disclose the necessary information. Only if the person under investigation continues to pose a threat to the public's health and fails to comply with public health recommendations or authorize public health to take necessary steps would the identity be released and then only if authorized by the Commissioner and consistent with Virginia law ([Va. Code § 32.1-36.](#))
- iii) It is the policy of VDH not to, on its own initiative, release the names of businesses under investigation to the public unless the business fails to comply with public health recommendations and continues to pose a risk to the public's health. Prior to such a release, VDH personnel must have the concurrence of OCOM and the business should be notified of VDH's intent to share the information. Additionally, as a state agency, VDH is subject to the FOIA and therefore, any document in VDH's possession is open to public inspection upon request unless a statutory exception applies. The medical records exception protects health information, and an exception for trade secrets might protect documents such as a restaurant's recipes, but the law does not contain an exception for the identity of the business. Therefore, if faced with a FOIA request for the identity of a business, VDH will need to comply unless an applicable FOIA exclusion exists. Other situations, such as a subpoena or a court order, could also mandate VDH disclosing a business' identity.
- iv) Sometimes releasing the name of a business is necessary to identify and contact persons who are at risk of illness because of an exposure associated with the business. In these situations, public health staff will need to discuss the matter with VDH senior leadership (respective Deputy Commissioner) prior to releasing the information to explain the public health need to take this action.
- d) Other Governmental Agencies
- i) VDH often works with other local, state, and federal agencies in the course of conducting [public health investigations](#). VDH staff must extend the confidentiality policy to those interactions and disclose information only when it is necessary for the investigation. Examples would be discussing a patient's test order or results with the Division of Consolidated Laboratory Services (DCLS) or discussing a particular child's illness with a school nurse. Disclosures of confidential information should not be necessary in investigations involving other state agencies with which VDH commonly partners (e.g., Virginia Department of Agriculture and Consumer Sciences, Virginia Department of Environmental Quality, Virginia Department of Emergency Management, Virginia Department of Game and Inland Fisheries, Virginia Department of Social Services) unless required as a mandated reporter to report instances of suspected abuse to DSS (Adult and Child Protective Services) pursuant to the Va. Code § [63.2-1603](#) through 1610 and Va. Code § [63.2-1509](#).
- ii) If a VDH staff person is concerned about practices being conducted by a private licensed provider, such information should be communicated through the chain of command to VDH senior management. At times, it might be necessary for VDH to discuss such cases with the Virginia Department of Health Professions (DHP) and/or file complaints with DHP.

## CONFIDENTIALITY

- iii) Most communications with federal agencies, such as CDC, USDA and FBI, in the course of [public health investigations](#) do not require the sharing of confidential information, unless required by law (e.g., regulatory reporting to the National Practitioner Databank). If an agency is partnering with VDH on an investigation, i.e., on site working together, then providing them access to confidential information collected as part of the investigation cannot always be avoided. Such federal partners should be advised of the importance of protecting confidentiality and local/state VDH co-investigators should ensure that federal partners do not copy or take confidential information back to their home base offices. For example, federal co-investigators must remove identities from information sheets and data files before they take them from the investigation site.
- iv) The Code of Virginia allows VDH to share information with CDC and state and federal law enforcement agencies in investigations involving the release, theft or loss of a dangerous microbe or pathogen, i.e., a select agent ([§32.1-36.F.2](#)), and to State Police for disease thought to possibly be the result of exposure to an agent or substance used as a weapon ([§32.1-39.B.](#)).
- e) Court orders and subpoenas
  - i) VDH staff receiving a court order or subpoena related to a public health investigation should consult the Office of the Commissioner immediately and division representative with the Office of the Attorney General (OAG) if a legal question exists.
  - ii) Generally, for a subpoena, the identities or identifying information of patients and providers must be removed unless the request comes from the patient or provider and the response contains only information pertaining to that individual or the request includes a signed waiver from the individual. Consultation with the OAG is usually required in these cases to come to an agreement with the requestor to redact identifying information.
  - iii) Court orders may require the release of certain confidential information; before releasing the requested information, the office or district shall seek advice from the Office of the Commissioner and/or the OAG as determined by the respective Deputy Commissioner.
- f) Media
  - i) VDH staff shall never release the name or personally identifying information of any patient or provider to the media. If a name is already publicly reported, VDH staff shall neither confirm nor deny the identity and shall instead inform the requestor that the Code of Virginia does not permit our disclosing identities. Providing other information that could inadvertently identify an individual, such as particular diagnosis, date of illness onset or death, and details about occupation, etc. must also be avoided.
  - ii) When there is media interest in individual, non-fatal or fatal cases, e.g., a novel influenza case or a pediatric influenza-associated death, VDH will report no detailed information beyond the age group of the patient and the health-planning region of residence. The age groups to be used are as follows: preschool (age 0-4 years), young school age (age 5-12 years), teenage (age 13-17 years), young adult (age 18-24 years), adult (age 25-64 years),

## CONFIDENTIALITY

and older adult (65 years of age or older). If a program uses other standard age groups, such age groups may be substituted for the ones listed above as long as the groups are broad enough to ensure that the identity of an individual cannot be deduced from the information. The five health planning regions are Central, Eastern, Northern, Northwest, and Southwest. This practice applies when the media are interested in reporting specific information about one or more certain individuals due to the individual's experience with a particular disease. Media requests for statistical information shall be handled according to the procedures outlined below, pertaining to statistical reports.

- iii) Communication about deaths that fall under the jurisdiction of the Office of the Chief Medical Examiner (OCME) will be handled by that Office. When other VDH Districts or Offices are involved with a medical examiner's case, the Office of the Chief Medical Examiner is responsible for releasing any public information that is necessary and will do so in coordination with the district/office. An example is release of information related to deaths suspected to be infectious in nature. OCME shall make every possible effort to protect confidentiality in accordance with this policy, their office-level procedures, and relevant legal mandates.
- iv) VDH may confirm the name of a facility or business to the media if necessary to protect the public's health, and if the media have already reported the name. If the media have not already obtained and reported the name of the facility or business, VDH should notify, and ideally seek permission from, the facility before releasing that information and only release information if it is necessary for the protection of the public's health.
- g) Other
  - i) If a facility alerts its constituents that it is involved in an outbreak but does not specify any additional details about the outbreak, a public health investigator may, after discussion with the facility, respond to inquiries about the nature of the illness and measures that can be taken to protect health.
  - ii) In the course of an outbreak investigation and due to the changeable nature of outbreak situations, public health investigators should avoid, to the extent possible, providing statistical information about the outbreak to the public. No legal authority exists, however, to protect the information. If attempts to protect the information are not successful, the investigator must aggregate the information in a way that assures that no individual can be identified.

### **7) Procedures for Protecting Confidential Information in Statistical Reports and Publications**

- a) Providing statistical information about the health of communities is a key function of public health. Therefore, public health authorities routinely release aggregate data on health indicators. The goal is to achieve a balance that maximizes the usefulness of the data and protects confidentiality. The rule of thumb is to release the minimum level of detail necessary to accomplish the objective.

## CONFIDENTIALITY

- b) All who prepare reports for release outside the agency are responsible for reviewing the report prior to release and evaluating the risk of identifying individuals. Factors relevant to the evaluation are the population size, the number of affected individuals, and the rarity and specificity of the health outcome being reported upon. If an individual could potentially be identified through the report, additional measures need to be applied to protect identities, such as cell suppression for small numbers. At a minimum, the direct supervisor of the person who prepared the report should review the report prior to its release.
  - c) Counts of events (e.g., frequency of non-fatal or fatal cases) may be released at the city or county level in response to requests for statistical information or in VDH statistical reports. To ensure that reports do not reveal confidential information inadvertently, cross-tabulated data at the city and county level, particularly for rare events, must be carefully scrutinized. Releasing multiple cross-tabulations at the jurisdiction level (i.e., number of cases of a rare disease by age, sex and race/ethnicity) should be avoided to the extent possible. If very specific information needs to be released to protect public health, e.g., when recommending interventions for a specific disease in a defined at-risk population, then the Office or District Director, as appropriate, must approve the release.
  - d) To protect the identity of individuals in statistical reports, staff may apply a "Rule of 5" for numerators. The "Rule of 5" states that cells with numerators greater than 0 and less than 5 may require aggregation with other cells or may be suppressed entirely if data are presented at or below the city/county level. For data provided at or below the city/county level, care should also be taken to ensure that the denominator is large enough to protect the identity of the individuals.
    - i) The National Center for Health Statistics provides a detailed description of guidelines for avoiding inadvertent disclosures in published tabular data on pages 15 through 17 of the Center's "Staff Manual on Confidentiality" at <http://www.cdc.gov/nchs/data/misc/staffmanual2004.pdf> (Hyattsville, MD, September 2004).
  - e) VDH staff may publish articles in scientific journals or present information at professional conferences that involve a case study or case series analysis that includes more detailed demographic or clinical information if necessary to advance scientific knowledge about a topic. Precautions should be taken in these instances, however, including: ensuring that the level of detail that is presented is necessary to convey the public health message; internal VDH peer-review occurs; and Office or District Director level of approval is granted. Whenever possible, signed consent by the person or legal representative of the person whose case is being described in a case study should be obtained prior to submitting the material to a journal or conference.
- 8) Procedures for Protecting Confidential Information in Research Requests**
- a) VDH has developed policies and procedures to ensure that the rights and welfare of human subjects involved in research are protected and consistent with both State (12 VAC 5-20-10) and Federal (45 CFR Part 46) regulations.

## CONFIDENTIALITY

- b) Any data collected and/or released for research purposes should comply with the policies of the VDH Institutional Review Board (IRB), and should have a research protocol with prior IRB approval. Information about VDH's IRB is available at <http://www.vdh.virginia.gov/healthpolicy/policyanalysis/irb.htm>
- c) Whenever VDH personnel receive a request for data that consist of individual records of persons captured in public health surveillance systems or included in [public health investigations](#), the need for an IRB review should be considered. If there is any question about whether IRB approval is needed, it is best to err on the side of caution and ask the requestor to submit the protocol and data request to VDH's IRB. The researcher must justify the need for confidential information or potentially identifiable individual data records and explain how confidentiality will be protected and data destroyed upon completion of the project.

### **8) Senior Leadership Notification**

- a) Information about certain public health situations needs to be communicated to VDH Senior Management using the [VDH Event Notification form](#). These situations include those where a large number of persons are ill, illness of unusual severity is occurring, risk of exposure to a serious agent is high, or the situation has the potential to become public or to be politically sensitive. When considering whether notification of senior management should occur, VDH staff should err on the side of caution and inform senior management. Such communication should be relayed through the chain of command in a manner that protects confidentiality.

## CONFIDENTIALITY

### IV. Administrative Procedures for the Protection of Human Resources Workforce Confidential Information

The provisions of this section apply to any VDH personnel who are involved in handling confidential human resources related information. **All VDH personnel involved in handling confidential human resources related information must review this section of the Confidentiality Procedures.**

#### Summary of Use

- Policies and procedures for protection of human resources workforce confidential information have been developed by the Department of Human Resource Management (DHRM) and Office of Human Resource (OHR), as outlined in the following table.
- VDH staff who handle human resource records must take the required training.

#### **1) Purpose**

The VDH has a legal and ethical obligation to protect the confidentiality of human resource records. This document, in conjunction with DHRM policies, establishes the framework for VDH staff to handle or manage human resource records which contain [personal information \(PI\)](#) and [protected health information \(PHI\)](#).

According to DHRM [Policy Number 6.05](#) - Personnel Records Disclosure, PI is defined as 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. Personal information includes name, race, sex, age, home address, home telephone number, marital status, dependents' names, insurance coverage, and social security number. The term does not include routine information maintained for the purpose of internal office administration; nor does the term include real estate assessment information.

#### **2) Procedures for Protection of Human Resources Workforce Confidential Information**

The following procedures relate to the management and disclosure of confidential information as well as prohibited activities. Violation of the relevant confidentiality policies and procedures may result in disciplinary action, up to and including, termination of employment and may also result in legal action.

- a) Maintenance of Records
  - i) [DHRM Policy # 6.10 - Personnel Records Management](#)
  - ii) [OHR Guidance - Personnel Records Management](#)
  - iii) OHR Confidential Information Listing

## CONFIDENTIALITY

**b) Disclosure**

- i) Personnel records are generally excluded from a duty of disclosure, consistent with Virginia’s Freedom of Information Act – See Code of Virginia § [2.2-3705.1](#) (1)
- ii) See [DHRM Policy # 6.05 - Personnel Records Disclosure](#)

**c) Prohibited Activities**

- i) Access or attempt to access information that is unrelated to job duties.
- ii) Access or attempt to access PHI beyond authorized [HIPAA](#) access level.
- iii) Disclose to any other person, or allow any other person to have access to any information that is proprietary or confidential and/or pertains to applicants, employees (including former employees), students, clients/patients, or the public, in violation of human resource policies and/or law. Disclosure of information includes, but is not limited to, discussions, fax transmissions, social networking sites, electronic mail messages, voice mail communication, written documentation, “loaning” computer access codes, and/or another transmission or sharing of data.

**d) Specific types of human resource files and the corresponding DHRM and VDH policies are summarized in the table below:**

File Type	Included Information	Authority
Personnel File	Original application and offer letter with acceptance	<a href="#">DHRM Policy # 6.10</a> - Personnel Records Management
	Background Investigation final report	
	Transactions	
	Employee Work Profile (Position description not confidential)	
	Performance Evaluations with Notice of Extraordinary Contributor or Notice of Improvement	
	Disciplinary Written Notices	
	Benefits (other than health)	
	Certification/Qualification (e.g., required training and/or licensure)	
Medical File	Miscellaneous – Such as policy sign-offs, Outside Employment, Telecommuting, Alternate Work Schedule	<a href="#">DHRM Policy # 6.10</a> - Personnel Records Management, VDH Personnel Records Management Guidance March 20,2008
	Health Benefits	
	Employee Health Records (e.g., exams, treatment, etc)	
	Workers' Compensation Claims (Placed in sealed envelope)	
	Employee Assistance Program (EAP) documents (Placed in sealed envelope)	
	Family and Medical Leave Act (FMLA) (Placed in sealed envelope)	
	Virginia Sickness and Disability Program (VSDP) (Placed in sealed envelope)	
Americans With Disabilities Act (ADA) accommodations (Placed in sealed envelope)		
Supervisor File	Documentation regarding employees' work performance or performance evaluation	<a href="#">DHRM Policy # 6.10</a> - Personnel Records Management
	Documentation of counseling sessions with employees on such things as performance or behavior problems or department policies and procedures	
	Interim performance evaluations	
	Copies of annual evaluations	
	Copies of Written Notices	
	Letters or memoranda from other sources regarding employees' job performance such as letters of commendation or complaint	
Copies of Attendance records		

## CONFIDENTIALITY

File Type	Included Information	Authority
	Copies of training certificates and/or other training records	
	Copies of position descriptions (Not confidential) and performance standards	
	Copies of agency personnel forms used to initiate personnel transactions	
Recruitment and Selection File	Position description (Not Confidential) Records related to recruitment efforts (Not Confidential) Copies of advertisements (Not Confidential) Employment applications Race and gender data on all applicants for Recruitment Management System (RMS) Screening and Selection criteria applied (Not Confidential) Screening documentation Interview questions and notes on applicant responses Work samples References and/or letters of recommendation Any documentation supporting selection or addressing non-selection Documentation supporting the salary determination	<a href="#">DHRM Policy # 2.10</a> - Hiring, VDH Policy # 2.10 - Recruitment & Selection
Payroll File	Deductions, garnishments, tax forms, time sheets	Library of VA Records Retention and Disposition Schedule No. 102
Background Investigation (BI)	Records of arrests, convictions, investigations, or security clearance information	<a href="#">DHRM Policy # 6.10</a> - Personnel Records Management, VDH Policy # 2.10.1 Background Investigation Program
Employment Eligibility Verification	I-9 forms	<a href="#">DHRM Policy # 6.10</a> - Personnel Records Management, VDH Policy # 2.10.2 Employment Eligibility Verification
Employee Training Records	Training records	<a href="#">DHRM Policy # 6.10</a> - Personnel Records Management
Employee Leave Records to include Leave Sharing	Leave records	<a href="#">DHRM Policy # 6.10</a> - Personnel Records Management
Exit Interviews		<a href="#">DHRM Policy # 6.10</a> - Personnel Records Management
Unemployment Compensation material		<a href="#">DHRM Policy # 6.10</a> - Personnel Records Management
Grievance Records		<a href="#">DHRM Policy # 6.10</a> - Personnel Records Management
Discrimination Complaint Case Files		<a href="#">DHRM Policy # 6.10</a> - Personnel Records Management
Workplace Violence Incident Reports & Court Protective Orders		<a href="#">VDH Policy # 1.80</a> - Workplace Violence

## CONFIDENTIALITY

### V. Administrative Procedures for the Protection of Federally Classified Information

The provisions of this section apply to any VDH personnel who are involved in handling federally classified information. Sensitive but unclassified information is also addressed for informational purposes. **All VDH personnel with federal clearances must review this section of the Confidentiality Procedures.**

#### Summary points for managing federally classified information

- Determine whether federal security clearance is needed. Employees who need clearance but do not have it should discuss the need for such clearance with their supervisor.
- Define the necessary training related to handling federally classified information and complete such training.
- If clearance and training are current, identify security classification of information being handled
- Determine proper handling process (includes with whom to share, communication channel permitted, location requirements and equipment needs based on level of classification).
- Ensure that information is handled accordingly and reach out to VDH senior leadership if special resources are required.
- If storage of information is required, identify storage capabilities based on level of classification.

#### Purpose

VDH has a legal and ethical obligation to protect classified information. The purpose of this document is to describe the classified information process as it applies to VDH personnel.

#### 2) Introduction

VDH, as a member of the Virginia Emergency Response Team (VERT), has a key role in homeland security. Key VDH emergency preparedness and response personnel have federal clearances obligating them to handle federally classified material consistent with legal requirements. Personnel without federal clearances also have an obligation to be familiar with their limitations as it relates to classified and other federally sensitive information.

#### 3) Classified Information

Classified information is defined as national security information that has been so designated pursuant to the three levels of classification as defined in Executive Order 12958, Classified National Security Information (NSI), and referred to as Top Secret, Secret, or Confidential (HHS Personnel Security /Suitability Handbook, 1998; available at [http://www.hhs.gov/asa/ohr/manual/files/98\\_1.pdf](http://www.hhs.gov/asa/ohr/manual/files/98_1.pdf)). In addition, according to [Executive Order 13526](#) "Classified National Security Information" (dated December 29, 2009, as amended), classified

## CONFIDENTIALITY

information is information determined to require protection from unauthorized disclosure, based on the damage to national security that could reasonably be expected to occur if the information were compromised. The damage could be “exceptionally grave”, “serious”, or just “damage” to national security.

The Executive Order has 8 categories or subject areas for NSI. These categories are the following:

- a) Military plans, weapons systems, or operations;
- b) Foreign government information;
- c) Intelligence activities/sources/methods or cryptology;
- d) Foreign relations including confidential sources.
- e) Scientific, technological or economic matters related to national security;
- f) Programs for safeguarding nuclear materials and facilities;
- g) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, protection services, relating to national security;
- h) Development, production, or use of weapons of Mass Destruction.

Regardless of the 8 subject areas mentioned above, NSI is categorized into 1 of 3 levels, based upon the expected damage if that information were released. All other notations deal with the access to and controls on dissemination (e.g., Special Compartmented Information or SCI). These levels and the respective damage are the following:

- a) Top Secret: “Exceptionally grave” damage
- b) Secret: “Serious” damage
- c) Confidential: “Damage”

**Only federal officials designate information as “Classified Information”.** VDH does not create anything at the state or local level that would be considered classified information in the federal sense of the term, regardless of the title that VDH staff place on the information.

Classified information is the property of the U.S. Government. When access to the classified information is granted by federal officials, the persons or agencies with that access are required to follow federal laws and regulations. Rarely, VDH is granted access to classified information. When VDH does have access to this information, it is primarily categorized as Confidential or Secret. Each of these titles indicates some sort of sensitive information that requires protection from disclosure to persons without appropriate clearance. Each of these may enjoy some exception from disclosure under the [Freedom of Information Act](#), depending upon the content of the material. Federally classified documents under VDH possession may be subject to FOIA unless we are able to cite a specific statute exempting them from FOIA. Consultation with the OAG would be necessary in such cases.

Classified information cannot be shared with anyone who does not hold the appropriate security clearance and security clearance is granted only by federal officials. Having a security clearance does

## CONFIDENTIALITY

not guarantee approved access to all classified information. Federal requirements for access to national security classified information include the following:

- a) Successful completion of the requisite background investigation required for the level of access;
- b) A “need to know” (see Need-to-know Principle and Responsibilities, below) in order to do the job;
- c) Having signed a Classified Information Non-Disclosure Agreement (SF-312);
- d) Having received a briefing about the responsibilities associated with access to classified information.

Although entire documents may be classified, individual paragraphs and elements within the document may be unclassified and must be marked accordingly by the federal agency responsible for the information. Markings include the following:

- a) (U/FOUO): Unclassified/ For Official Use Only
- b) (U/FOUO/LES): Unclassified/ For Official Use Only/ Law Enforcement Sensitive
- c) (C): Confidential
- d) (S): Secret
- e) (TS): Top Secret
- f) NOFORN: paragraphed marked (S/NOFORN). Note that NOFORN is for intelligence information that may not be passed to foreign nationals.
- g) SECRET//ORCON: Dissemination and Extraction of Information Controlled by Originator (ORCON) or (OC). Any additional distribution or inclusion in another document must be approved by originator of the document. Used on intelligence information that could permit identification of a sensitive intelligence source or method.
- h) SECRET//ORCON, PROPIN: Proprietary Information Involved (PROPIN) or (PR) is used with or without a security classification. Identifies information provided by a commercial firm or private source under an express or implied understanding that the information will be protected as a trade secret or proprietary data with actual value; Similar to PCII.
- i) SECRET//REL TO USA, EGY, GBR: Authorized for Release to \_\_\_\_ (REL TO) signifies intelligence information that is releasable to or has been released through proper disclosure channels to the named foreign government or international organization.
- j) ORCON: paragraphed marked (S/OC)
- k) PROPIN: paragraphed marked (S/PR)
- l) REL TO: paragraphed marked (S/REL TO)

#### 4) **Sensitive But Unclassified Information (SBU)**

SBU is a designation of information in the federal government that, though unclassified, often requires strict controls over its distribution. SBU is a broad category of information that includes material covered by other designations. The following are examples of various classifications used

## CONFIDENTIALITY

by different government agencies to denote information that is considered “sensitive” but unclassified (SBU):

- a) For Official Use Only (FOUO)
- b) Limited Official Use (LOU)
- c) Official Use Only (OUO)
- d) Law Enforcement Sensitive (LES)
- e) Sensitive Security Information (SSI)
- f) Protected Critical Infrastructure Information (PCII)
- g) Governor’s Confidential Working Papers

These categories of information are considered sensitive and require a “need-to-know” for access as well as protection against unauthorized disclosure. Sensitive (Unclassified) information may be shared only with those with a “need to know”.

For Official Use Only (FOUO) is the marking used by the U.S. Department of Homeland Security (DHS) to identify Sensitive but Unclassified information within the DHS community, the unauthorized disclosure of which could adversely impact a person’s privacy or welfare, the conduct of Federal programs, or other operations essential to the national interest and that is not otherwise covered by a statute or regulation.

Other government agencies and international organizations frequently use different terms to identify sensitive but unclassified information, such as “Limited Official Use (LOU),” “Official Use Only (OUO),” and in some instances “Law Enforcement Sensitive (LES).” In most instances the safeguarding requirements for this type of information are equivalent to FOUO.

Other agencies and international organizations may have additional requirements concerning the safeguarding of their sensitive information. When available, follow the safeguarding guidance provided by the other agency or organization. Should no guidance be available, the information will be safeguarded in accordance with the FOUO guidance provided in this document. It is not permitted to mark Information as FOUO to conceal government negligence, ineptitude, or other disreputable circumstances concerning to a government agency.

### **5) Need-to-know Principle and Responsibilities**

Need-to-know is one of the most fundamental security principles. Need-to-Know is the determination made by an authorized holder of classified information that access to the information is required by another appropriately-cleared individual in order to perform official duties. The practice of need-to-know limits the damage that can be done by a trusted insider who becomes no longer trustworthy. Failures in implementing the need-to-know principle have contributed greatly to the damage caused by a number of recent espionage cases. The need-to-know principal imposes a dual responsibility on the employee and all other authorized holders of classified information. When performing job duties, the employee is expected to limit requests for information to those with a genuine need-to-know. Under some circumstances, the employee may be expected to explain and

## CONFIDENTIALITY

justify the need-to-know after asking others for information. Conversely, the employee must ensure that anyone who is given classified information has both a legitimate need to know the information and the appropriate clearance to receive that information. The person to whom the information request is made is obliged to ask the requestor for sufficient information for determining his/her need-to-know. The requestor of the information is obliged to justify their need-to-know. In situations where there is uncertainty as to whether a person has a need-to-know, the employee should contact the originator of the information for clarification or consult with the U.S. Department of Homeland Security (DHS) Office of Security (OS) Administrative Security Division (ASD).

Adhering to the requirements of “need-to-know” is sometimes difficult because it conflicts with our natural desire to be friendly and helpful. However, its importance cannot be overstated and each person with access to classified information must maintain a level of self-discipline and responsibility to ensure that this principal is followed. Two specific circumstances in which the employee needs to be particularly careful about the “need-to-know” are described below.

- a) An individual from another organization may contact you and ask for information about classified information which you possess. Even though you have confirmation that the person has the appropriate security clearance, you are also obliged to confirm the individual’s need-to-know before providing information. If you have any doubt, contact the information’s originator or consult with DHS OS/ASD.
- b) Difficult situations sometimes arise when talking with friends who used to be assigned to the same program where you are now working. The fact that a colleague used to have a need-to-know about this program does not mean he or she may have access to the information. There is no "need" to keep up to date on sensitive developments after being transferred to a different assignment.

### 6) Declassifying Information

In addition to the “Need to Know” principle, there is also the principle of “Requirement to Share”. For information to be truly useful to the vast majority of officials and responders, information needs to be in an unclassified form whenever action is needed. To declassify or downgrade the information’s classification, the originating federal agency takes the original document and creates versions of the document with lower levels of classification. For example, a federal agency might create a “Top Secret” report that reveals the source of the information. A “Secret” version might be created that would not reveal the source, but might give explicit detail on the threat. A “Sensitive but Unclassified” version might be created that would contain only the necessary action the recipient agencies should take given their specific roles. Similarly, when the Fusion Center, for example, receives a classified document and wants to create an unclassified version for dissemination, they will make a request to the agency from where the information originated for releasing an unclassified version of the document; this request and document revision process takes time and is not always successful.

### 7) Marking of Classified Documents

## CONFIDENTIALITY

Classified information and sensitive but unclassified information should be appropriately labeled or marked to achieve the following:

- a) Alert the holder to presence of national security information (NSI);
- b) Indicate the assigned classification level;
- c) Identify special security requirements, if any;
- d) Advise the holder of protection required;
- e) Identify the source of classification; and
- f) Indicate the duration of protection.

Requirements for marking the documents are as follows:

- a) Overall page markings;
  - i) Highest level on the page, or
  - ii) Highest level of the entire document
- b) Portion markings;
- c) Classification block;
  - i) "Classified By" line
  - ii) "Derived From" line
  - iii) "Downgrade to"
  - iv) "Declassify On" line; some agencies have exemptions

### 8) **VDH Procedures**

The following procedures are described in more detail, below.

- a) Procedures for Accessing and Disseminating Classified Materials at VDH
- b) Procedures for Appropriately Marking Classified Information
- c) Procedures for Storing Classified Information
- d) Procedures for Destroying Classified Information
- e) Procedures for Appropriately Marking FOUO Information
- f) Procedures for Storing FOUO Information
- g) Procedures for Destroying FOUO Information
- h) Procedures for Accessing and Disseminating FOUO Information at VDH
- i) Procedure for Reporting of Compromises of Classified or FOUO Information

### 9) **Procedures for Accessing , Handling and Disseminating Classified Materials at VDH**

If you are unsure what to do, ask for assistance. There are people who can help; they are from VDH, the Fusion Center, the Secretary of Veterans Affairs and Homeland Security (formerly Office of Commonwealth Preparedness - OCP) and at the federal agency that sponsors the employee's clearance.

- a) Access
  - i) To gain access to classified information, you must have the appropriate clearance and you must demonstrate that you have a need to know the information. Both requirements **must** be met; satisfying only one requirement is not sufficient.

## CONFIDENTIALITY

- ii) You must verify clearance. Secretary of Veterans Affairs and Homeland Security (SVAHS) maintains a list of DHS-cleared state staff, the Fusion Center maintains a list of cleared staff and the agency that sponsored the subject's clearance can verify a clearance using procedures that are in place. Someone simply stating "Yes, I have a clearance" is not adequate verification. A piece of paper that says a person has a clearance is not adequate.
  - iii) The security officer or security point of contact from the sponsoring federal agency for that person can verify the clearance.
  - iv) You must verify the need to know: the holder of the information must be satisfied that the potential recipient really does need the classified information to perform the job or assist with whatever the situation involving the classified material requires.
- b) Handling and Disseminating Classified Information
- i) Classified information may not be transmitted or reproduced by unsecured means. Personal or Virginia government e-mail systems should not be used for disseminating classified information. Land line or mobile phones should not be used when discussing classified information. Unclassified printers, fax, computers or copiers should not be used when reproducing classified information.
  - ii) All personnel are reminded that just because classified information appears in the public domain it does not mean that the information has been declassified by proper authority. [Executive Order 13526](#), "Classified National Security Information," Section 1.1.(c) states, "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." Therefore, in accordance with this order and current DHS policy, personnel should not use any unclassified system to access, download or attempt to download from a public web site any information that is believed to be classified, nor should they comment or confirm the degree of sensitivity of such information, or discuss the content in a potentially classified document with persons who would not otherwise be authorized access.
  - iii) Classified Working Papers include classified meeting notes, Information you have put together from other classified sources or any Classified Secret or Confidential document you create. These working papers can be hand written. Working papers must have the name of the creator, the date that the document was created, the Level of Classification marked clearly at the top and bottom and the declassify date. Within 180 days of its creation date classified working papers must be destroyed or must be formally classified as a final document.
  - iv) To safeguard classified information, it is important to protect the information from observation or advertisement.
    - (1) Cover sheets should be used when not in a secure container.
    - (2) The information should be placed in an unmarked envelope or file folder when the handler is walking the halls.
    - (3) It is recommended to establish a Clean-desk policy and implement end-of-day checks for unsecured classified documents and for storage container and lock inspections.

## CONFIDENTIALITY

- (4) An SF-702 form should be filled out daily on the document safe, regardless of whether or not the safe was opened during the day.
- v) When discussing classified information on the telephone, a secure Telephone Exchange (STE) is needed.
  - (1) STE consists of a normal telephone that has a special card installed to make it secure.
  - (2) Security clearance is required for STE and the STE must occur in an approved space.
  - (3) Crypto cards are assigned to one STE; if you mix them up, the card becomes useless.
  - (4) Cards shall be stored in an approved container when not in use and periodic updates are required (Rekey).
  - (5) When using STE, the physical environment should be secured, such that doors should be closed and remain locked, blinds or curtains should be closed, blackberry and cell phones should be stored in another area, and someone with a clearance must be outside the room to make sure no one is listening.
- vi) For classified conversations that take place outside certified secure areas, the following procedures must be followed.
  - (1) All persons must be cleared for information with a Need to Know.
  - (2) The conversation must be in an approved space.
  - (3) Cell Phones, blackberry, and, internet enabled devices shall not be present.
  - (4) Doors must be closed and remain locked and blinds or curtains should be closed.
  - (5) Before the conversation begins, someone must announce the HIGHEST LEVEL of classified information to be discussed (Must say "this is Classified at ...").
  - (6) Area has to be sponsored by DHS; an approved DHS Multi-use Security Survey Form for SLTPS Programs required.
  - (7) Only good for verbal discussions –no amplified sound or video teleconferencing allowed.
  - (8) The host must implement security procedures and put them in place for the meeting, including an attendee roster and a sufficient number of cleared staff to carry out security functions.
  - (9) In Richmond, approved spaces include the Fusion Center, OCP Conference Room, National Guard secure room and FBI office.

### **10) Procedures for Appropriately Marking Classified Information**

VDH will be the recipient of such information and will not be expected to mark classified information

### **11) Procedures for Storing Classified Information**

- a) All Classified Material must be locked in a GSA-approved container when not in use.
- b) The combination for the container should be memorized (i.e., not written) and combinations should be changed as necessary. Combinations are classified information in and of themselves. Use Open/Closed indicators.
- c) Crypto cards for secure telephones and video units must be locked up when not in use.
- d) If you forget to lock or store classified information appropriately, the event should be reported as soon as possible.

## CONFIDENTIALITY

### **12) Procedures for Destroying Classified Information**

- a) Always shred obsolete documents, only in approved shredders.
- b) Files should be audited every six months and obsolete documents should be purged accordingly.

### **13) Procedures for Access to and Dissemination of FOUO Information at VDH**

- a) A security clearance is not needed for access to FOUO information. Access to FOUO information is based on a "need-to-know" as determined by the holder of the information. Where there is uncertainty as to a person's need-to-know, the holder should request dissemination instructions from their next-level supervisor or the originating activity.
- b) FOUO information may be shared with other agencies (e.g., Federal, state, tribal, private sector, or local government and law enforcement officials), provided that a need-to-know has been established and the information is shared as part of official governmental activity, to include homeland defense, and no dissemination restrictions have been cited by the originator.
- c) FOUO information may be transmitted via non-secure fax machine; however, use of a secure fax is encouraged. Where a non-secure fax machine is used, the sender will ensure that a recipient is present at the time of the fax transmission and that the materials faxed will not be left unattended or subject to unauthorized disclosure.
- d) FOUO information may be transmitted over official email channels. However, it shall not be sent to personal email accounts. For added security when transmitting FOUO information by email, password protected attachments may be used with the password transmitted or otherwise communicated separately.
- e) FOUO information may be mailed by regular US Postal Service first class mail or any commercial mailing service.
- f) FOUO information may **not** be entered or posted on any public website.

### **14) Procedures for Appropriately Marking FOUO Information**

Information determined to be FOUO must be sufficiently identified so that persons granted access to it are aware of its sensitivity and protection requirements.

- a) At a minimum, on the bottom of each page "FOR OFFICIAL USE ONLY" should be inserted.
- b) Materials containing specific types of FOUO information can be further marked with an applicable caveat, e.g., "LAW ENFORCEMENT SENSITIVE," to alert the reader of the type of information conveyed.
- c) Additional access and dissemination restrictions may also be cited as the situation warrants. Markings typically associated with classified information such as originator information, downgrading instructions, and date/event markings are not required on FOUO documents.

### **15) Procedures for Storing FOUO Information**

- a) When unattended, FOUO information shall be stored in a locked filing cabinet, locked desk drawer, a locked overhead storage compartment such as systems furniture credenza, or a similar locked compartment.

## CONFIDENTIALITY

- b) Information can also be stored in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without the need-to-know, such as a locked room or an area where access is controlled by a guard, cipher lock, or card reader.

### **16) Procedures for Destroying FOUO Information**

- a) Hard copy FOUO materials must be destroyed by shredding, burning, pulping, or pulverizing, that is sufficient to assure destruction beyond recognition and reconstruction.
- b) Agency electronic storage media shall not be used to store or transit federal classified material.
- c) After destruction, materials may be disposed of with normal waste.
- d) Electronic storage media shall be sanitized appropriately by overwriting or degaussing and according to the Commonwealth of Virginia Standard (SEC514: Removal of Commonwealth Data from Electronic Media), VDH Information Security Policy, and applicable HIPAA standards.
- e) Paper products or electronic media containing FOUO information shall not be disposed of in regular trash or recycling receptacles unless the materials have been destroyed as specified above.

### **17) Procedures for Reporting of Compromises of Classified or FOUO Information**

Compromise, suspected compromise and suspicious or inappropriate requests for classified or FOUO information must be reported to the originator of the information and up the supervisory chain as soon as possible. For security violations, the SVAHS is the Commonwealth Point of Contact (POC) for security issues. All violations should be reported to the POC and DHS as soon as they happen and without delay or attempts at covering up the incident.

## CONFIDENTIALITY

### VI. Resources

#### **Federal Laws and Regulations**

Among the key statutes of the U.S. government that include specific reference to the confidentiality of health data are the following:

- Section 308(d) of the Public Health Service Act (42 U.S.C. 242m). Confidentiality protections afforded to the health data acquired by the National Center for Health Statistics supersede any rights granted to the public or to individuals by either the Federal Freedom of Information Act or the Privacy Act of 1974.
- Freedom of Information Act (5 U.S.C. 552)
- Confidentiality of Alcohol and Drug Abuse Patient Records, Final Rule August 10, 1987 (42 CFR part 2)
- The National Research Act, Public Law 93-348, enacted July 12, 1974. Federal regulations 45 CFR 46 implement this law for the protection of human subjects from research risks and establish the principles for the operation of Institutional Review Boards.
- Special Supplemental Food Program for Women, Infants and Children, Section 17 of the Child Nutrition Act of 1966, as amended. WIC Program Consolidated Regulations, January 1995. 246.26(d) Confidentiality. WIC Program - General Administration: Confidentiality USDA FNS, FNS Instructions 800-1. 7 C.F.R. 246.26
- Health Care Financing Administration: Release of Information: Medicaid (42 CFR 432.306 et seq., and 431.301 et seq.)
- [FERPA](#) (Family Education Rights and Privacy Act) 34 CFR 99
- Older Americans Act (42 U.S.C. 3001 as amended)
- [HIPAA](#) Privacy Rule – 45 CFR Parts 160 and 164. USDHHS summary is available at the following link:  
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html>  
HIPAA Description of What [Protected Health Information](#) Includes:  
<http://www.hipaa.com/2009/09/hipaa-protected-health-information-what-does-phi-include/>
- Specific federal grants may include their own requirements (Title X, Title V, Ryan White, for example)

#### **Code of Virginia TITLE 32.1 – Health Laws**

Key statutes of the Code of Virginia that include specific references to health data are listed below. For specific information, see <http://leg1.state.va.us/000/src.htm>.

- § 32.1-36. Reports by physicians and laboratory directors
- § 32.1-36.1. Confidentiality of test for human immunodeficiency virus; civil penalty; individual action for damages or penalty
- § 32.1-38. Immunity from liability
- § 32.1-39. Surveillance and investigation
- § 32.1-41. Anonymity of patients and practitioners to be preserved in use of medical records

## CONFIDENTIALITY

- § 32.1-45.2. Public safety employees; testing for blood-borne pathogens; procedure available for certain citizens; definitions
- § 32.1-46. Immunization of children against certain diseases; authority to share immunization records, Virginia Immunization Information VIIS
- § 32.1-48.015 Authorization to disclose health records in isolation/quarantine cases
- § 32.1-64.2. Confidentiality of records; publication; Commissioner required to contact parents, physicians, and relevant local early intervention program
- § 32.1-67.1. Confidentiality of records; prohibition of discrimination
- § 32.1-69. Records confidential; disclosure of results of screening
- § 32.1-69.2. Confidentiality of records; publication; authority of Commissioner to contact parents and physicians
- § 32.1-71. Confidential nature of information supplied; publication; reciprocal data-sharing agreements
- § 32.1-83. Inclusion and exclusion of drug products and vendors; protection of trade secret information
- § 32.1-111.3. Statewide emergency medical care system
- § 32.1-116.1 Prehospital patient care reporting PPCRs
- § 32.1-116.1:1. Disclosure of medical records
- § 32.1-116.2. Confidential nature of information supplied; publication; liability protections
- § 32.1-125.5 Confidentiality of Complainant's identity
- § 32.1-126.01 Dissemination of criminal background check information
- § 32.1-127.1:03 Virginia Health Records Privacy Act
- § 32.1-127.1:04 Use of certain [protected health information](#)
- § 32.1-127.1:05 Notification of breach of medical information notification
- § 32.1-137.16 Records of utilization review
- § 32.1-137.2. Certification of quality assurance; application; issuance; denial; renewal
- § 32.1-137.4. Examination, review or investigation
- § 32.1-137.5. Civil penalties; probation; suspension; restriction or prohibition of new enrollments to managed care health insurance plan licensee; revocation or nonrenewal of certificate of quality assurance; appeal process; correction
- § 32.1-138.5 Confidentiality of complainant's identity
- § 32.1-163.3 Identities of persons making certain reports to remain confidential
- § 32.1-271 Disclosure of information in vital records
- § 32.1-276.9 Confidentiality of patient level data
- § 32.1-283.4. Confidentiality of certain information and records collected and maintained by the Office of the Chief Medical Examiner
- § 2.2-3705.5. Health exclusions to Virginia's Freedom of Information Act (<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-3705.5>)

## CONFIDENTIALITY

### *Virginia State Board of Health Regulations*

Key chapters within the Virginia State Board of Health Regulations that relate to the protection of confidential information are presented in the table below. For specific information, see <http://townhall.virginia.gov/>

VAC Code	Chapter Title
<a href="#">12 VAC 5-11</a>	Public Participation Guidelines
<a href="#">12 VAC 5-20</a>	Regulations for the Conduct of Human Research
(a) <a href="#">12 VAC 5-31</a>	Virginia Emergency Medical Services Regulations
<a href="#">12 VAC 5-66</a>	Regulations Governing Durable Do Not Resuscitate Orders
<a href="#">12 VAC 5-67</a>	Advance Health Care Directive Registry
<a href="#">12 VAC 5-71</a>	Regulations Governing Virginia Newborn Screening Services
<a href="#">12 VAC 5-80</a>	Virginia Hearing Impairment Identification and Monitoring System
<a href="#">12 VAC 5-90</a>	Regulations for Disease Reporting and Control
<a href="#">12 VAC 5-105</a>	Rabies Regulations
<a href="#">12 VAC 5-110</a>	Regulations for the Immunization of School Children
<a href="#">12 VAC 5-115</a>	Virginia Immunization Information System Regulations
<a href="#">12 VAC 5-120</a>	Regulations for Testing Children for Elevated Blood-Lead Levels
<a href="#">12 VAC 5-125</a>	Regulations for Bedding and Upholstered Furniture Inspection Program
<a href="#">12 VAC 5-140</a>	Notices of Establishment and Description of Seasonally Condemned Areas At Marina Facilities
<a href="#">12 VAC 5-150</a>	Regulations for the Sanitary Control of Storing, Processing, Packing or Repacking of Oysters, Clams and Other Shellfish
<a href="#">12 VAC 5-160</a>	Regulations for the Sanitary Control of the Picking, Packing and Marketing of Crab Meat for Human Consumption
<a href="#">12 VAC 5-165</a>	Regulations for the Repacking of Crabmeat
<a href="#">12 VAC 5-170</a>	Prohibiting the Taking of Fish for Human Consumption From the North Fork of the Holston River
<a href="#">12 VAC 5-191</a>	State Plan for the Children with Special Health Care Needs Program
<a href="#">12 VAC 5-195</a>	Virginia Women Infants and Children Program Regulations
<a href="#">12 VAC 5-200</a>	Regulations Governing Eligibility Standards and Charges for Health Care

## CONFIDENTIALITY

	Services to Individuals
<a href="#">12 VAC 5-215</a>	Rules and Regulations Governing Health Data Reporting
<a href="#">12 VAC 5-216</a>	Methodology to Measure Efficiency and Productivity of Health Care Institutions
<a href="#">12 VAC 5-217</a>	Regulations of the Patient Level Data System
<a href="#">12 VAC 5-218</a>	Rules and Regulations Governing Outpatient Data Reporting
<a href="#">12 VAC 5-220</a>	Virginia Medical Care Facilities Certificate of Public Need Rules and Regulations
<a href="#">12 VAC 5-230</a>	State Medical Facilities Plan
<a href="#">12 VAC 5-371</a>	Regulations for the Licensure of Nursing Facilities
<a href="#">12 VAC 5-381</a>	Home Care Organization Regulations
(b) <a href="#">12 VAC 5-391</a>	Regulations for the Licensure of Hospices
<a href="#">12 VAC 5-405</a>	Rules Governing Private Review Agents
<a href="#">12 VAC 5-407</a>	Regulations for the Submission of Health Maintenance Organization Quality of Care Performance Information
<a href="#">12 VAC 5-408</a>	Regulation for the Certificate of Quality Assurance of Managed Care Health Insurance Plan (MCHIP) Licensees
<a href="#">12 VAC 5-410</a>	Rules and Regulations for the Licensure of Hospitals in Virginia
<a href="#">12 VAC 5-411</a>	Regulations for Inpatient Hospital Licensure
<a href="#">12 VAC5-412</a>	Regulations for Licensure of Abortion Facilities
<a href="#">12 VAC 5-421</a>	Food Regulations
<a href="#">12 VAC 5-431</a>	Sanitary Regulations for Hotels
<a href="#">12 VAC 5-440</a>	Regulations for Summer Camps
<a href="#">12 VAC 5-450</a>	Rules and Regulations Governing Campgrounds
<a href="#">12 VAC 5-460</a>	Regulations Governing Tourist Establishment Swimming Pools and Other Public Pools
<a href="#">12 VAC 5-462</a>	Swimming Pool Regulations Governing the Posting of Water Quality Results
<a href="#">12 VAC 5-475</a>	Regulations Implementing the Virginia Organ and Tissue Donor Registry
<a href="#">12 VAC 5-481</a>	Virginia Radiation Protection Regulations

## CONFIDENTIALITY

<a href="#">12 VAC 5-490</a>	Virginia Radiation Protection Regulations: Fee Schedule
<a href="#">12 VAC 5-501</a>	Rules and Regulations Governing the Construction of Migrant Labor Camps
<a href="#">12 VAC 5-508</a>	Regulations Governing the Virginia Physician Loan Repayment Program
<a href="#">12 VAC 5-510</a>	Guidelines for General Assembly Nursing Scholarships
<a href="#">12 VAC 5-520</a>	Regulations Governing the State Dental Scholarship Program
<a href="#">12 VAC 5-530</a>	Regulations Governing the Virginia Medical Scholarship Program
<a href="#">12 VAC 5-540</a>	Rules and Regulations for the Identification of Medically Underserved Areas in Virginia
<a href="#">12 VAC 5-542</a>	Rules and Regulations Governing the Virginia Nurse Practitioner/Nurse Midwife Scholarship Program
<a href="#">12 VAC 5-545</a>	Guidelines for the Nurse Educator Scholarship
<a href="#">12 VAC 5-550</a>	Board of Health Regulations Governing Vital Records
<a href="#">12 VAC 5-570</a>	Commonwealth of Virginia Sanitary Regulations for Marinas and Boat Moorings
<a href="#">12 VAC 5-590</a>	Waterworks Regulations
<a href="#">12 VAC 5-600</a>	Waterworks Operation Fee
<a href="#">12 VAC 5-610</a>	Sewage Handling and Disposal Regulations
<a href="#">12 VAC 5-611</a>	Onsite Sewage Regulations
<a href="#">12 VAC 5-612</a>	Regulations for the Onsite Sewage Indemnification Fund
<a href="#">12 VAC 5-613</a>	Regulations for Alternative Onsite Sewage Systems
<a href="#">12 VAC 5-615</a>	Regulations for authorized onsite soil evaluators
<a href="#">12 VAC 5-620</a>	Regulations Governing Application Fees for Construction Permits for Onsite Sewage Disposal Systems and Private Wells
<a href="#">12 VAC 5-630</a>	Private Well Regulations
<a href="#">12 VAC 5-640</a>	Alternative Discharging Sewage Treatment Regulations for Individual Single Family Dwellings
<a href="#">12 VAC 5-650</a>	Schedule of Civil Penalties

## CONFIDENTIALITY

### VDH

#### Virginia Department of Health General Confidentiality Agreement

I acknowledge that I have received and maintained current training on the VDH Confidentiality Policy and Procedures and it is my responsibility to comply with all aspects of the policy and procedures. I acknowledge and understand that I may have access to confidential information, including [Protected Health Information \(PHI\)](#), and [Personal Information \(PI\)](#) regarding VDH personnel, clients/patients, or the public. In addition, I acknowledge and understand that I may have access to proprietary or other confidential information or business information belonging to the VDH. Therefore, except as required or permitted by law, I agree that I will not:

- Access or attempt to access confidential data that is unrelated to my job duties at VDH;
- Access or attempt to access Protected Health Information (PHI) beyond my stated authorized [HIPAA](#) access level;
- Disclose to any other person, or allow any other person access to, any information related to VDH that is proprietary or confidential and/or pertains to employees, students, clients/patients, or the public. Disclosure of information includes, but is not limited to, verbal discussions, FAX transmissions, electronic mail messages, voice mail communication, written documentation, "loaning" computer access codes, and/or another transmission or sharing of data.
- Disclose Protected Health Information (PHI) in violation of law.

I understand that VDH and its employees, clients/patients, or others may suffer irreparable harm by disclosure of proprietary or confidential information and that VDH may seek legal remedies available to it should such disclosure occur. I understand that violations of this agreement may result in disciplinary action, up to and including, termination of my employment. Further, I understand that I am bound by this agreement after I am no longer an employee, volunteer, contractor, or assignee of VDH.

---

Employee Signature

Date

---

Supervisor's Signature

Date

## CONFIDENTIALITY

### Policy Administration

**Original Policy Date:** January 10, 2012  
**Last Revision Date:** June 30, 2015  
**Policy Review Cycle:** June 30, 2017

**Reviewer:** Signature on File 7/15/15  
Richard P. Corrigan, Date  
Deputy Commissioner for Administration

**Approver:** Signature on File 7/15/15  
Marissa Levine, MD MPH Date  
State Health Commissioner

**Contact, General Provisions:** David Trump, MD MPH  
Chief Deputy Commissioner, Public Health & Preparedness  
David.trump@vdh.virginia.gov  
804-864-7026

**Contact, Direct Patient Care:** Jodie Wakeham  
State Nursing Director  
[Joanne.Wakeham@vdh.virginia.gov](mailto:Joanne.Wakeham@vdh.virginia.gov)  
804-864-7017

**Contact, PH Investigations:** Diane Woolard  
Division of Surveillance and Investigation Director  
[Diane.Woolard@vdh.virginia.gov](mailto:Diane.Woolard@vdh.virginia.gov)  
804-864-8124

**Contact, Human Resources:** Micah Fairchild  
HR Division Director: Policy & Systems Improvement  
Micah.fairchild@vdh.virginia.gov  
804-864-7087

**Contact, Federally Classified Information:** Robert Mauskapf  
Office of Emergency Preparedness Director  
[Bob.Mauskapf@vdh.virginia.gov](mailto:Bob.Mauskapf@vdh.virginia.gov)



Office of the Commissioner  
VDH Policy Number: OCOM #1.01  
Effective Date: 05/9/2012  
Last Revision Date: 07/10/2015  
Review Cycle: 08/01/2017

Reviewer: Deputy Commissioner for Administration

## CONFIDENTIALITY

804-864-7035

**Contact, Automated Data Security:**

Debra Condrey  
Chief Information Officer  
[Debbie.condrey@vdh.virginia.gov](mailto:Debbie.condrey@vdh.virginia.gov)  
804-864-7118

**Contact, Information Security Officer:**

Wes Kleene  
Information Security Officer  
[Wes.Kleene@vdh.virginia.gov](mailto:Wes.Kleene@vdh.virginia.gov)  
804-864-7111

**Contact, HIPAA Privacy Officer:**

Doug Harris  
VDH Privacy Officer  
[Doug.Harris@vdh.virginia.gov](mailto:Doug.Harris@vdh.virginia.gov)  
804-864-7007