



Office of the Commissioner
VDH Policy Number: 01.07.101
Effective Date: 05/9/2012
Last Revision Date: 08/17/2021
Next Review Cycle: 08/17/2024

Confidentiality Policy

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

Security and confidentiality of Confidential Information is of the utmost importance at VDH. It is the responsibility of all VDH personnel to respect and maintain the security and confidentiality of Confidential Information. A violation of this policy may result in disciplinary action.

This policy is intended to provide VDH personnel with a basic understanding of their responsibilities to protect and safeguard the confidential Information to which they have access as a result of their employment.

For purposes of this policy, "Confidential Information" is defined as information disclosed to VDH personnel or known to VDH personnel as a consequence of their employment at VDH, and not generally known outside VDH, or is protected by law. Examples of "Confidential Information" include but are not limited to – student grades; financial aid information; social security numbers; payroll and personnel records; health information; self-restricted personal data; credit card information; information relating to intellectual property such as an invention or patent; research data; passwords and other IT-related information; and VDH financial and account information. Individual offices, departments, or programs may have additional types or kinds of information that are considered "Confidential Information" and are covered by this policy. "Confidential Information" includes information in any form, such as verbal, written documents or records, or electronic data.

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. 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 and the OCOM 01.07.115 HIPAA policy. Specifics regarding the handling of electronic confidential data are contained in those documents.



Office of the Commissioner
 VDH Policy Number: 01.07.101
 Effective Date: 05/9/2012
 Last Revision Date: 08/17/2021
 Next Review Cycle: 08/17/2024

Confidentiality Policy

Policy

It is the policy of VDH to protect confidential information. ***Confidential information includes*** Protected Health Information (PHI) ***and*** Personally Identifiable 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

VDH personnel **shall have the following responsibilities under this 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 shall collect no more confidential information than is reasonably necessary to accomplish their work-related tasks.

VDH personnel will not seek to obtain any Confidential Information involving any matter which does not involve or relate to the person's job duties. Confidential Information or VDH records, documents, or other information may not be maliciously tampered with, altered, or destroyed.

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, and the authorized individuals shall be provided the minimum necessary information needed for performing their job duties.

VDH personnel will not remove materials or property containing Confidential Information from their department or program area unless it is necessary in the performance of the person's job



Office of the Commissioner
VDH Policy Number: 01.07.101
Effective Date: 05/9/2012
Last Revision Date: 08/17/2021
Next Review Cycle: 08/17/2024

Confidentiality Policy

duties. Any and all such materials, property, and Confidential Information are the property of VDH. If materials or property containing Confidential Information are removed from VDH, VDH personnel must safeguard the materials/property and control access as necessary. This responsibility to safeguard and control access to materials and property similarly applies to any telework/remote access situation as provided in VDH Telework Policy. Upon termination of any assignment or as requested by VDH personnel's supervisor, VDH personnel will secure all such materials/property and copies thereof or return all such materials/property and copies to their supervisor or supervisor's designee. Safeguarding shall comply with all VDH security policies and confidentiality procedures #01.07.101P.

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.

If VDH personnel has any question relating to appropriate use or disclosure of Confidential Information, they shall consult with their supervisor or other appropriate VDH personnel.

In the case of a health or safety emergency, relevant Confidential Information may be disclosed as necessary to appropriate individuals in order to perform their job duties.

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 annual data privacy and security 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.



Office of the Commissioner
VDH Policy Number: 01.07.101
Effective Date: 05/9/2012
Last Revision Date: 08/17/2021
Next Review Cycle: 08/17/2024

Confidentiality Policy

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 confidentiality procedures #01.07.101P 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. 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.

9. 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 personnel responding to requests for access to patient medical records and subpoenas is posted on the FOIA page of the VDH internal website

10. 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.**

11. Training

Training is available and required for VDH personnel on the handling and use of confidential records during orientation, through the required on-line TRAIN Course, the Annual Cybersecurity Awareness HIPAA Course, **and** on-the-job training by supervisor. VDH personnel



Office of the Commissioner
VDH Policy Number: 01.07.101
Effective Date: 05/9/2012
Last Revision Date: 08/17/2021
Next Review Cycle: 08/17/2024

Confidentiality Policy

routinely handling said information must renew their knowledge of the policy every three years in keeping with the review cycle. Supervisors are responsible for seeing that training is completed.

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

Authority

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

Related Policies, Procedures, and/or Resources

[01.07.101 Confidentiality Procedures with Confidentiality Policy Acknowledgement](#)
[OCOM 1.15 HIPAA Policy](#)
[VDH HIPAA Page](#)
[Commonwealth's SEC501 Security Standard](#)
[Commonwealth's SEC514: Removal of Commonwealth Data from Electronic Media](#)
[Commonwealth IT Security Standards and Information Security Policies](#)
[State Library of Virginia Records Retention](#) (relating to confidential records)
[Health Insurance Portability and Accountability Act \(HIPAA\)](#)
[Freedom of Information Act \(FOIA\)](#)
[VDH FOIA page](#)
[VDH Telework Policy](#)
[Information Security Program Guide](#)
[VDH Information Security Policy](#)
[VDH Acceptable Use Policy](#)
[Social Media Policies](#)

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



Office of the Commissioner
 VDH Policy Number: 01.07.101
 Effective Date: 05/9/2012
 Last Revision Date: 08/17/2021
 Next Review Cycle: 08/17/2024

Confidentiality Policy

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 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.



Office of the Commissioner
VDH Policy Number: 01.07.101
Effective Date: 05/9/2012
Last Revision Date: 08/17/2021
Next Review Cycle: 08/17/2024

Confidentiality Policy

6. Personally Identifiable Information (PI)

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

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 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



Office of the Commissioner
VDH Policy Number: 01.07.101
Effective Date: 05/9/2012
Last Revision Date: 08/17/2021
Next Review Cycle: 08/17/2024



Confidentiality Policy

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.

Policy Approval

Reviewer:	DocuSigned by:  <small>F1E1BD5BA7654B6...</small>	8/17/2021 3:44:13 PM EDT
	Tiffany Ford Deputy Commissioner for Administration	Date
Approver:	DocuSigned by:  <small>E9883CE3DE124C6...</small>	8/17/2021 3:47:28 PM EDT
	M. Norman Oliver State Health Commissioner	Date

Contact, General Provisions: Parham Jaberi
 Chief Deputy Commissioner, Public Health and Preparedness
 parham.jaberi@vdh.virginia.gov
 (804) 864-7025

Contact, Direct Patient Care: Jeannine Uzel
 State Nursing Director
 jeannine.uzel@vdh.virginia.gov
 804-864-7014

Contact, PH Investigations: Caroline Holsinger
 Division of Surveillance and Investigation Director
 caroline.holsinger@vdh.virginia.gov
 804-864-8111



Office of the Commissioner
VDH Policy Number: 01.07.101
Effective Date: 05/9/2012
Last Revision Date: 08/17/2021
Next Review Cycle: 08/17/2024

Confidentiality Policy

Contact, Human Resources:	Jennifer Ferguson HR Division Director: Policy & Systems Improvement jennifer.ferguson@vdh.virginia.gov 804-864- 7105
Contact, Federally Classified Information:	Robert Mauskapf Office of Emergency Preparedness Director bob.mauskapf@vdh.virginia.gov 804-864-7035
Contact, Automated Data Security:	Suresh Soundararajan Chief Information Officer suresh.soundararajan@vdh.virginia.gov 804-864-7140
Contact, Information Security Officer:	Stephanie Williams-Hayes Chief Information Security Officer stephanie.williams-hayes@vdh.virginia.gov 804-864-7111
Contact, VDH Privacy Team:	Douglas Harris VDH Privacy Officer doug.harris@vdh.virginia.gov 804-864-7007 Kimberly Johnson HIPAA Compliance Officer kimberly.howardjohnson@vdh.virginia.gov 804-864-7342



Office of the Commissioner
VDH Policy Number: 01.07.101
Effective Date: 05/9/2012
Last Revision Date: 08/17/2021
Next Review Cycle: 08/17/2024

Confidentiality Policy

Policy History

EFFECTIVE DATE	DESCRIPTION
05-09-2012	Policy established.
8-17-2021	Policy reformatted and procedures separated into new document. Language was updated to make current. Review cycle changed to three years.