# Security and Confidentiality Policies and Procedures

# For Non-DDP Staff

Division of Disease Prevention

Office of Epidemiology

Virginia Department of Health

2025

# Table of Contents

## Revision History

| Version | Date | Description of Changes |
|---|---|---|
| 1 | 9/9/2020 | Original Document |
| 2 | 8/20/2021 | Updated Least Privileges section |
| 3 | 9/10/2021 | Revised for non-DDP staff |
| 4 | 9/18/2025 | Reformatted Appendices<br>Updated Phone, Fax and Address in Attachment 1<br>Added Verification of Receipt Form as Attachment 3 |

## Preface

The Division of Disease Prevention (DDP) is one of six divisions within the Office of Epidemiology (OEPI) at the Virginia Department of Health (VDH). DDP's mission is to maximize public health and safety through the elimination, prevention, and control of disease, disability, and death caused by HIV/AIDS, viral hepatitis and other sexually transmitted infections. The DDP Security and Confidentiality (S&C) Policies and Procedures for Non-DDP Personnel are based upon the security and confidentiality requirements outlined by the Centers for Disease Control and Prevention (CDC). These policies incorporate and reference existing VDH policies related to the security and confidentiality of public health data. All agency personnel must annually review the Security and Confidentiality Policies and Procedures and acknowledge their agreement to abide by these policies electronically. Emails prompting agency personnel to complete electronic acknowledgement of these policies are sent in November and must be completed by December 31 of the same year.

## Purpose

This document reflects security and confidentiality requirements for agency personnel whose jobs require handling of confidential information in relation to an active agreement with DDP. Agency personnel who engage with confidential public health information must safeguard these data at all times. These policies facilitate the secure physical and electronic collection, storage, and use of data while maintaining confidentiality. Maintaining the confidentiality of patient-level data is the responsibility of each agency working with DDP. The DDP Security and Confidentiality Policies and Procedures for Non-DDP Personnel is a living document (changing as needed) and is subject to change. Always refer to the most recent version of this document, and talk with your contract monitor if you have questions about the material covered in this document.

## Key Terms/Glossary

**Access:** Ability or means needed to read, write, modify, or communicate data/information.

**Access controls:** Cohesive set of procedures designed to ensure that anyone with access to identifiable public health data:

1. Is the person he or she claims to be (authentication),
2. Has a verified public health need to have access to the data in question, and
3. Has been authorized to access the data and is doing so from an authorized place using an authorized process.

**Advanced Encryption Standard (AES):** This standard specifies the algorithm that can be used to protect electronic data and is issued by the National Institute of Standards and Technology (NIST). Publication 197 of the Federal Information Processing Standards (FIPS) (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf ) contains the specifications of the AES, which can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back to its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. NIST publication 140-2 details the protection of a cryptographic module within a security system necessary to maintain the confidentiality and integrity of the information protected by the module http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf .

**Aggregated data:** Information—usually summary statistics—that might be compiled from personally identifiable information (PII) but is grouped so as to preclude identification of individual persons.

**Analysis dataset:** Set of aggregated data created by removing identifying information (e.g., names, addresses, ZIP codes, telephone numbers) so that the data cannot be linked to a specific person but can still be used for data analysis.

**Authorized access:** Permission granted to an authorized person to see confidential or potentially identifiable public health data, based on the public health role of the individual and their need to know.

**Authorized person:** Person who has been granted authorized access to confidential information to carry out assigned duties.

**Breach:** A departure from established policies or procedures, or a compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or loss of control of PII. A breach is an infraction or violation of a policy, standard, obligation, or law. A breach is a confirmed privacy and/or security threat that will compromise the sensitive data, hardware, or information system. A breach in data security would include any unauthorized use of data, even aggregated data without names. Breaches are mitigated by the VDH Privacy and Security teams. For examples of PHI and PII refer to the attachment, "What Is PHI and PII?".

**Breach of confidentiality:** A breach, as defined above, that results in the release of PII to unauthorized persons (i.e., employees or members of the general public).

**Breach of Personally Identifiable Information:** Defined by the Office of Management and Budget (OMB) Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII, whether physical or electronic.

**Confidential information:** Any private information about an identifiable person who has not given consent to make that information public.

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

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

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

**Data steward:** Person responsible for ensuring that data used or stored in an organization's computer systems are secure, classified appropriately, and used in accordance with organizational policies.

**Disclosure:** Occurs when identifiable information concerning an individual is made known to a third party. Disclosures may be *authorized* (as when a person has consented to the information being so divulged), *unauthorized* (as when information is intentionally revealed to a party not consented to by the person), or *inadvertent* (as when a tabulation or file is unintentionally made available to the public that reveals or can be used to reveal personal information).

**Encryption:** Manipulation or encoding of information so that only parties intended to view the information can do so. The most commonly available encryption systems involve public key and symmetric key cryptography. In general, for both public and symmetric systems, the larger the key, the more robust the protection.

**HIPAA Compliance Officer:** The individual responsible for providing guidance and management of HIPAA compliance in accordance with DHHS OCR regulations and the VDH HIPAA Policy.

**Identifiable data or identifiable information:** See *Personally Identifiable Information.*

**Incident:** An incident is an attempted, or successful, unauthorized access, use, disclosure, modification, destruction, or interference with system operations. Internal incidents are due to a departure from following policies and procedures. Incidents are mitigated by the VDH Privacy and Security teams. Although incidents are a violation of operational policies and procedures, incidents are not privacy or security threats to the sensitive data, hardware, or an information system.

**Information security:** Protection of data against unauthorized access. Effective security measures are always a balance between technology and personnel management.

**Information Security Officer:** An individual responsible for developing, maintaining, and managing the VDH Information Security Program in order to meet or exceed the requirements of the Commonwealth's IT Security Standards.

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

**Management controls:** Controls that include policies for operating information technology resources and for authorizing the capture, processing, storage, and transmission of various types of information. They also may include training of agency personnel, oversight, and appropriate and vigorous response to infractions.

**Personnel controls:** Personnel controls, such as training, separation of duties, and background checks, that are used as part of information security and management controls.

**Personally Identifiable Information (PII):** Information that allows the identity of a person to be determined with a specified degree of certainty. This could be a single piece of information or several pieces of data which, when taken together, may be used to identify an individual. Therefore, when assembling or releasing analysis data sets, it is important to determine which fields, either alone or in combination, could be used to identify a person and which controls provide an acceptable level of security.

**Protected Health Information (PHI):** The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule provides federal protections for PHI held by covered entities and gives patients an array of rights with respect to that information. The Privacy Rule does permit the disclosure of PHI needed for patient care and other important purposes.

# Confidentiality

### A. Health Insurance Portability and Accountability Act (HIPAA)

HIPAA privacy regulations created national standards for the protection of medical record privacy and other personal health information. The United States Department of Health and Human Services (HHS) issued the HIPAA regulations and the Office of Civil Rights is responsible for implementation and enforcement.

- HIPAA privacy regulations limit how Protected Health Information (PHI) is shared, prevents employers from using PHI in employment decisions and requires employers to establish confidential safeguards for PHI handling.
- The HIPAA Privacy Rule defines what PHI is and how it can be used and disclosed.
- The HIPAA Security Rule identifies the required and addressable security implementations to control how PHI is accessed and disclosed.
- HIPAA contains both civil and criminal penalties for violations of the regulations. The HIPAA Omnibus Rule makes business associates of covered entities directly liable for compliance with certain HIPAA Privacy and Security Rules' requirements.
- Further information about HIPAA regulations is available at the HHS website (Health Insurance Portability and Accountability Act of 1996 | ASPE).

### B. VDH Confidentiality Policy (OCOM #1.01)

The VDH Confidentiality Policy (updated 2021) covers the handling of all confidential information while also balancing VDH's responsibility to protect public health. Confidential information includes PHI and personally identifiable information (PII) regarding employees, clients/patients, and the public, as well as other forms of confidential information related to proprietary and/or business information. Confidential information is usually encountered by VDH personnel carrying out the following activities:

- Providing clinical/patient care services
- Conducting public health investigations
- Accessing public health records
- Managing human resource records
- Processing accounts payable and receivable
- Accessing governmental classified information

Key components of the VDH Confidentiality Policy include the following:

1. Limit collection of confidential information
2. Limit use of confidential information
3. Limit Access to confidential information
4. Limit disclosure of confidential information

5. Acknowledgement of confidentiality policy and procedures
6. Data destruction
7. Publications and reports based on confidential information
8. Security
9. Data integrity
10. Compulsory legal process, requests from law enforcement, and Freedom of Information Act (FOIA) requests
11. Non-compliance

Components of the VDH Confidentiality Policy are incorporated throughout this document. Agency personnel are expected to review the complete policy available here.

### C. Minimizing Data Usage

Agency personnel must collect and share only the minimum amount of information necessary to conduct specified program activities.  Access controls regarding the need to access PHI must be followed.

- The purpose for which data is to be collected should clearly be stated when the data is to be shared or used.
- Do not simply collect data because it may be used at a later date or because it is easily accessible.
- Evaluate data prior to use to ensure accuracy and validity.
- If proposed data collection includes PII, ensure that such data is absolutely necessary.
- Use non-identifiable data for public health purposes whenever possible and distribute it in a timely manner.

### D. Concept of Least Privilege

The agency must maintain all patient-level information securely and confidentially, categorizing all patient records (paper and electronic) within the agency as "confidential."  Any confidential communication (written, verbal or electronic) should be shared with other persons on a strict need to know basis.

- Confidential information should be accessed only by a user with the authority to access such information, as delegated, and with an expressed need to access such information.
- Agency management  should ensure that users have least privilege and only the access necessary to perform job duties.  They should consider the following before granting a user with access to confidential information:
  - Is there a demonstrated business need for this user's access?

    - Is the user up-to-date with the agency's required training related to security and confidentiality?
    - Did the user review and acknowledge the non-DDP S&C Requirements in the current calendar year?
    - Has the user ever inappropriately handled confidential information?
- Appropriate written approvals are needed for any release of or access to confidential information.
- Sections 32.1-36.1.A, 32.1-38 and 32.1.41 of the *Code of Virginia* specifies when it is permissible to share confidential information with authorized individuals*,* based on an established need to receive such information.

## E. Sending Confidential Information Electronically

### i. Phone

Confidential information can be shared over the phone with authorized staff for purposes including morbidity reporting, record searching treatment or morbidity history, etc.  Assistance with sharing confidential information through incoming calls should only be completed if agency personnel are confident of the identity of the caller and he/she is an authorized recipient of such information.

#### Incoming Calls

- Agency personnel must choose an appropriate voicemail passcode, without common logic associated with the individual that could easily be guessed or learned by others.
- Uncertainty regarding the identity of a caller should be verified via a call back procedure and/or discussion with appropriate personnel.
- If a call back verification is performed, agency personnel should not acknowledge this procedure to the caller.
- The caller's name, location and telephone number should be obtained and the caller should be informed that agency personnel will return their call as quickly as possible.
- Any uncertainty regarding the caller's location or authorization to receive such information should be immediately forwarded to the appropriate supervisor or other designated member of agency management.
- Agency personnel should not release any information if unsure of the legitimacy or authorization of the caller.

#### Outgoing Calls

- Confidential information is shared with persons outside of the agency on a strict need to know basis and performed only in secure areas.
- Confidential information should only be shared on outgoing calls if the recipient is authorized to receive such information.  If placing an outgoing call to a patient, always ask

the patient to confirm their date of birth- at a minimum- before discussing any confidential information.

- Agency personnel must verify and document the legitimacy or authorization of the recipient before the release of any confidential information.
- Messages with identifying patient information or terms easily associated with surveillance or risk factors (for example, HIV, AIDS, STD, TB, VH or any specific behavioral information) should not be left on voicemail systems or via text messaging.
- Disclosure of confidential information by telephone must also be from a secure or private area. The use of personal cellular phones or public telephones to communicate confidential information is not allowed.

### ii. Fax

Incoming and outgoing fax transactions from the agency should follow the same guidelines. In the event a fax containing confidential information containing PHI is sent to the wrong number, inform your supervisor and follow instructions for reporting a HIPAA data breach. A fax cover sheet should be used for all faxes originating from the agency, and must include a confidentiality notice.

- Confidential information should be faxed with caution, using the utmost discretion.
    - Double check the fax number typed into the machine before sending.
    - Always obtain a send receipt from the fax machine showing the number that a fax was sent to.
- Faxed, confidential information must only be sent to, or received at, secure/confidential locations.
- When coordinating an incoming fax containing confidential information, agency personnel should 1) verify that the sender has the correct fax number, and 2) await the fax completion and immediately remove documents from the fax machine.
- If incoming faxes are not received within an expected time frame, the agency personnel awaiting the fax should contact the sender.
- Completed faxes with confidential information should not be left on fax machines unattended.

### iii. Email

- Agency personnel are prohibited from sending confidential information containing PII or PHI via unsecured email, either internally (between agency personnel) or externally (between agency personnel and outside sources, including VDH staff).
- Agency personnel may use an encryption service (e.g. Virtru) to send confidential information via encrypted email.
    - Encryption services provide end-to-end encryption on email messages and attachments. Recipients of emails sent using encryption must authenticate with the encryption service in order to decrypt the protected content. Encrypted emails will

not be readable by anyone other than the intended recipient. **The email subject field is not encrypted, so do not put PHI or PII content into the subject field.**

- Confidential information shall not be transmitted via unsecured email. Agency personnel who routinely encounter PHI in their normal job duties should include a reminder in their email signature reminding recipients against sending PHI or PII through unsecure email. This reminder should include the following language:
    - "Please do not reply to this email with any protected health information or patient identifying information. This includes: name, phone number, date of birth, address and medical record number. Please call my confidential line at (XXX)-XXX-XXXX to coordinate this exchange. Thank you."

### F. Secure File Transfer Protocol (SFTP)

Secure File Transfer Protocol or Secure FTP – sometimes abbreviated to SFTP, is a widely-recognized method of encrypting data or files during their transmission from one computer to another. Secure FTP is a generic term that encompasses a variety of encryption methods.

- SFTP can be used to send confidential files to colleagues, as well as large files (>25 MB) that are too big to attach to an email.
- Agency personnel who need to use SFTP should work with technical support at their agency to have the software installed on their computer. One recommended standard is a program called FileZilla, and is currently the standard for VDH.

### G. Using Data Systems Appropriately

Confidential data systems used by DDP and the agencies with whom we contract for services are maintained by data stewards in other Offices or Divisions within VDH, the CDC, or external vendors. Database access is structured with management and personnel controls to ensure access is based on the concept of least privilege. User accounts and rights are set up and maintained by the applicable Data Manager or designated back up. Any changes to user accounts must be approved by the appropriate VDH Director or their designee. VDH Data Managers review database account access for all other DDP systems containing PHI/PII at least quarterly and document the findings. User access for REDCap and  eHARS is reviewed on a monthly basis, while the ADAP and Maven databases are reviewed on a quarterly basis.

- Never share your data system log on credentials, including user identification codes and passwords.
- Never use access to a VDH-owned or acquired database to obtain information that is not immediately necessary for a work-related task you are authorized to complete. This includes database searches of family, friends, acquaintances, or any individual beyond the scope of your immediate work assignment.
- Any improper activity on a database observed should be reported to DDP and is subject to disciplinary action.

# Physical Security

### A. Building Access

The agency must ensure safeguards for accessing the organization's building for employees and visitors. Please refer to the HIPAA Security Standards for Physical Safeguards for HIPAA compliance requirements that address the physical security of facilities that contain protected health information (PHI).

- Employees are required to swipe their employee identification (ID) and/or sign in if scanning IDs are not available at the agency upon entering the building, accessing secure floors and file rooms.
- Employees should never allow anyone to follow them through secure access points without swiping their ID or signing in with a picture ID.
- Employees should display their ID at all times upon entering the building.
- Authorized visitors must check in at the entrance and be accompanied by an agency employee at all times.
- It is a Ryan White recommendation that operational hours be posted on the exterior of the building visible to the public.

### B. Storing Confidential Information

All confidential information should be stored in secure file rooms. Agency personnel must adhere to the following requirements when using confidential information:

- Only confidential documents needed to perform daily work should be removed from the file room.
- Return all confidential documents to their appropriate place within the file room.
- During business hours, confidential documents with PII must be secured in a locked file cabinet or rolling cart when the employee is away from their workspace.
- Never leave confidential documents in the workspace outside of normal business hours. Store locked rolling carts in the file room during non-business hours.
- Ensure that confidential files are not left on a desk or in view when clients or visitors are present.
- Only authorized users may enter file rooms to retrieve or review confidential documents.

### C. Taking Confidential Information into the Field

Certain agency personnel may need to transport confidential information during assignments in the field (away from the office). Agency personnel must adhere to the following requirements when taking confidential information from the office:

- Confidential information should only be removed from the office with prior supervisory approval and for the purposes of conducting official business.
- Locked containers provided by the employer must be used to transport confidential information.
- All confidential information transported from the office is the responsibility of the agency personnel until all records are returned to their secure location at the office.
- Laptops, flash drives, and locked containers containing confidential information must be in the agency personnel's possession at all times (e.g. do not leave unattended in a vehicle)

### D. Taking Confidential Information to Other Areas of the Agency's Building

Documents containing confidential information must occasionally move from the assigned, secure file room to other areas of the building. Agency personnel must adhere to the following requirements when taking confidential information to other areas of the building:

- Confidential information must only be moved from its assigned space in the file room to another location in the building for a legitimate public health business purpose approved by the employee's supervisor.
- Confidential documents must be placed in a folder, envelope, box, or other container so that the confidential information they contain is not visible to other employees who do not have a business need to view the information.
- Computers must be locked when the user steps away from their workstation. Computers on the Windows operating system can be locked by pressing the Windows + "L" keys on the keyboard.
- Privacy screen protectors may be required to prevent others from viewing confidential information on the user's computer screen in situations where the computer screen cannot be hidden from individuals without authorization to view confidential information.
- All confidential records must remain in the personal possession of the assigned agency personnel until the documents are returned to their secure location.
- All confidential records must be locked in a file cabinet or secured briefcase any time they are out of sight of the assigned employee.
- Contact information must be included on any item (folder, envelope, box) containing the confidential records in the event of loss or theft within the building. This information must include the employee's name, phone number, and email address. Avoid including a job title if it would provide an indication of what the briefcase may contain.

### E. Mail

The agency's programmatic forms containing PII may be sent and received via a secure mail system, provided the mailing is done in a confidential manner in accordance with the agency's mailing policy.

- Record a log of materials that are mailed using de-identified information (e.g. field record number, Maven ID number, etc).
- Two envelopes must be used when mailing forms containing PII:
  - Forms shall be placed inside the "first" envelope and securely sealed. The envelope must protect contents from being read or viewed, and a regular manila envelope will meet this requirement. The number and type of forms being sent shall be indicated on the outside of the inner envelope.
  - The "second" or outer envelope must be made of a material that is tear, puncture-, and moisture-resistant, such as Tyvek.
- The recipient's name and address, and VDH return address shall be placed legibly on both envelopes in the top left corner. Ensure the recipient's name and address are correct. If mailing PII forms to VDH, United Parcel Service (UPS) mailing labels for "return service" will be sent to HIV and STD testing sites. The UPS label shall be placed on the "second" or outer envelope. Double addressing gives an additional level of security that the package will reach the intended person/address.
- Mail shall be marked *"Confidential, To Be Opened By Addressee Only."*
- The frequency of mailing shall be at a minimum weekly; this will avoid the risk of overstuffed envelopes which could be damaged in transit. It is suggested that mailings be combined where activities are occurring in multiple clinics at the same location if the volume is typically low. If UPS service has not been established, a call for pick-up will be necessary.
- Notify the recipient when you have mailed the document and request that they notify you upon receipt.
- Immediately notify your supervisor in the event that items mailed do not reach the recipient, or the recipient reports that the envelope has been opened or severely damaged. Follow instructions for reporting a HIPAA data breach of personally identifiable information.

### F. Records Retention

STD, HIV, and VH morbidity records, interview records, field records, laboratory reports, service delivery records containing PHI/PII, and invoices are retained for surveillance-related and historical purposes based on requirements stipulated in the agency's contractual agreement with VDH and the Retention Schedules from the Library of Virginia (LVA). Once these records are no longer used by agency personnel on a daily basis, they must be securely stored or destroyed according to the age of the document. Consult the LVA Retention Schedules and/or your contract administrator for more information.

- All documents containing confidential information, including PII, must be destroyed using a commercial-quality cross-cutting shredder.
  - Large quantities of documents containing confidential information, including PII, may be shredded by an approved vendor. Daily shredding may be done, as

needed, by placing documents in a locked shred bin or using a shredding machine.
    - CD-ROMS containing PHI must be incinerated or physically broken, into several pieces, to be rendered unusable.

# Cyber Security (Electronic Data Security)

## A. Using electronic data safely

### i. Social Engineering

Social engineering is a manipulation technique that tricks people into disclosing confidential information. Forms of social engineering attacks can include email phishing or voice phishing. Email and voice phishing are cybercrimes in which someone poses as a legitimate institution in order to lure individuals into providing sensitive data. Any phishing attacks should be reported immediately to the agency's information security officer. Signs of email or voice phishing include:

- Emails or phone calls that create a strong sense of urgency.
- Emails that appear to be work-related but use a personal email address, such as @gmail.com, @yahoo.com, or @hotmail.com
- Emails or phone calls that contain language, tone, or a signature that is inconsistent with the supposed sender.
- Emails phone calls that pressure you to bypass or ignore our security policies.
- Emails or phone calls containing a generic greeting such as "Dear Customer".
- Emails or phone calls that contain offers that are too good to be true.
- Emails or phone calls that try to invoke curiosity or fear.

### ii. Encryption

Encryption protects information by making it unreadable or unusable by anyone that does not have your key or password.

- All PCs/laptops that are used in non-traditional work settings that may access confidential data must have encryption software installed (ex: Sophos SafeGuard or Guardian Edge for laptops or IronKey™ flash drives).
- All portable devices that receive, store, or transport PHI must incorporate the use of encryption software that meets standards detailed in FIPS Publication 197, *Advanced Encryption Standards (AES)*. It is recommended to use FIPS-140-2 level 3 encryption on all external drives.
- Before taking any device containing sensitive data out of a secured area, the data file(s) must be encrypted.
- Each user is responsible for ensuring such encryption software is included on their notebook/laptop/tablet.

- Data transferred to CDC must be encrypted using the AES 256 encryption method when any moderately or highly sensitive files, any moderately or highly critical information, or any limited access/proprietary information is being transmitted to or from CDC electronically.
- All agency personnel with installed encryption software are required to check refreshed/replaced machines to ensure all encryption software and security measures are on their current computer.

### iii. Teleworking

Teleworking is becoming increasingly common. When teleworking, PII should only be accessed using the agency's approved Virtual Private Network (VPN). The VPN uses encryption to secure all data sent through the internet, making the network virtually "private". A telework location must be in a private area with limited access when confidential information is accessed.

- Agency personnel must ensure that their home wifi devices or mobile hotspots have a secure password or phrase and use multi-factor authentication, when possible.
- The ability to observe any PII must be restricted to only the teleworker.
- Logging into confidential data systems and/or other files and data sources containing PII should be limited to an absolute need for such access while using the VPN. Such access should only be conducted in the absence of all other persons.
- Remote access to email, network files and/or data systems should not be left unattended at any time, regardless of circumstance, while using the VPN.
- Agency personnel should continue to electronically lock their computers when stepping away, as they would in the office.

### iv. Computer Workstation Accessibility

All users authorized to access PII are individually responsible for protecting their own workstation, laptop, and/or other devices. This responsibility also includes the protection of User Identifications, also called usernames or login names, and passwords/codes that would allow access to PII.

- Users may not share their access or give their credentials (user ID, password, pin, etc.) or other authentication information to anyone under any circumstances.
- Employees should ensure databases are closed and PCs are electronically locked when leaving the work area for any period of time including, but not limited to bathroom breaks, lunch breaks, and at the end of the business day.
- PC monitors must be situated such that they cannot be easily viewed by persons other than the user.
- All users are required to report any suspicious activity involving their PC immediately to their supervisor.

### v. Flash Drives

Encrypted flash drives, such as IronKey™, should be the only type of flash drive used to temporarily store or transfer confidential data. An IronKey™ will erase all data stored after 10 incorrect password attempts.

- All removable or external storage devices containing PII must include only the minimum amount of information needed to accomplish assigned tasks.
- Users should ensure that they include relevant contact information in the IronKey™ set up process in the event of loss of the device.
- Any IronKey™ containing confidential data must be maintained separately from a laptop and held securely when not in use. This helps to ensure that loss or theft of a laptop does not include an IronKey™ device.
- Decryption keys (i.e. IronKey™ passwords) must be maintained separately.
- Upon return of the IronKey™ when no longer needed and/or termination of employment, device passwords must be provided to the employee's supervisor.
- All users must take necessary precautions not to infect data-related software and hardware with computer viruses and not to expose equipment to extreme temperature variations. Necessary precautions include, but are not limited to:
  - Ensuring that flash drives, laptops, and other electronic equipment are never left in vehicles.
  - Not connecting flash drives and laptops to non-agency devices or networks.
- External storage devices should only be used for pre-authorized activities.

### vi. Web Conference Meetings

Several conference tools exist to host virtual meetings, like Cisco WebEx, Zoom, GoToMeeting, and Microsoft Teams. It is important to follow precautions when hosting or attending virtual meetings using these platforms.

- Do not make meetings public. Require a meeting password or use the waiting room feature to control admittance of attendees.
- Do not share a link to your meeting on an unrestricted, publicly available social media post. Instead, provide the link directly to the individuals you intend to invite.
- Manage your screen sharing options. Change screen sharing to "host only" to prevent attendees from sharing information on their screens which could have PII.
- Always use the most updated version of the conferencing software. Older versions may be susceptible to hacking.
- Best practices for security and privacy on popular conferencing tools are listed below
  - **Cisco Webex** https://help.webex.com/en-us/8zi8tq/Cisco-Webex-Best-Practices-for-Secure-Meetings-Hosts
  - **GoToMeeting** https://support.goto.com/meeting/help/security-faqs-g2m050014
  - **Microsoft Team** https://support.microsoft.com/en-gb/office/make-a-public-team-private-in-teams-6f324fbc-6599-4612-8daa-ff5d35a746bf
  - **Zoom** https://explore.zoom.us/docs/doc/Securing%20Your%20Zoom%20Meetings.pdf
  - **Google Meet** https://support.google.com/meet/answer/9852160?hl=en

# Plans, Policies and Procedures

### A. HIPAA Data Breaches

A HIPAA data breach is an instance in which an unauthorized release or access to PHI or PII has occurred. This applies whether the organization stores and manages its data directly or through a contractor such as a cloud service provider, or if internal safeguards are not active to protect the data.

A breach can be malicious in nature or purely unintentional. A security breach can take many forms including:

- Inadvertently sharing PHI or PII via misdirected emails, faxes, or documents
- Inadvertently allowing unauthorized persons to overhear conversations containing PHI or PII
- Not seeking a private location to hold conversations involving PHI or PII
- The loss, theft, or misplacing of equipment such as laptops, mobile phones, portable USB drives, documents, or files containing PHI or PII
- Negligence in the handling of medical files, lab results or reports without regard to privacy measures, or failing to use the appropriate physical safeguards, such as securing documents that contain PHI/PII; and
- Failing to protect systems or external drives with passwords or encryption, which leaves data vulnerable, such as not logging off your workstation when you will be away or at the end of your workday.

If the agency personnel or data owner believes that a data breach has occurred, they must take the following actions:

- Immediately notify your direct supervisor.
    - The user should complete the agency's Breach Incident Notification form, which will gather more details concerning the incident, including the user's contact information for the incident assessment.
    - As applicable, the Privacy Team will assist the Security Team in determining whether a breach has actually occurred, and if so, will take the following actions:
        - 1) Inform the ISO for collaborative action
        - 2) Provide instructions on securing the data
        - 3) Mitigate the effects, and
        - 4) Document actions taken to address the incident, preserve the evidence, and handle applicable breach reporting to the DHHS Office of Civil Rights, if needed.
- External incidents reported to VDH follow a similar remediation process but with additional collaboration with the external agency's privacy/security contact.
- For any known or suspected breaches involving Information Technology (IT), networking data systems, hardware, and/or software, the agency's ISO must also be notified.

### B. Security Incidents

A security incident is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system possesses, stores, or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. A security incident can take many forms.

Some examples of a security incident are:

- Loss, damage, theft, or improper disposal of equipment, documents, or files;
- Disclosing PII/PHI to a person who is not authorized to have it;
- Unauthorized access (e.g. agency personnel access PII they were not authorized to view);
- Any security situation that could compromise PII/PHI (e.g. computer virus, phishing email);
- Slow running computers or applications that are not performing correctly (this could be due to a virus or malware, and should be reported).

External agencies that suspect a breach of PHI or ePHI (electronic protected health information) should immediately report the matter to their VDH contact for the Privacy and Security teams breach intake and assessment. The breach incident assessment process begins when a staff member alerts the Privacy or Security Teams of a suspected breach and forwards the required Breach Incident Notification Form, which summarizes the details of the incident for investigation, whether internally or externally.

Breach Incident reports are also documented in the agency's Breach Incident Response Log for investigation and, if applicable, for notification to HHS Office of Civil Rights (OCR).

If the agency personnel or data owner believes that a security incident has occured, they must take the following actions:

- Upon discovery of an incident, immediately report it within 24 – 48hrs,
- Complete and return the agency Breach Incident Notification Form (attached) for incident assessment and response.
- Contact the agency ISO via phone and/or email.
- The ISO will conduct an initial response, engage privacy officers, complete the incident response form, conduct an investigation, conduct recovery and follow-up, and issue a final report to stakeholders. The ISO will consult with their manager, Agency Head, HIPAA Compliance Officer, and/or Internal Audit Director on incident and incident reporting to third party agencies.
- The ISO is responsible for reporting breaches within one hour of occurrence to the appropriate DDP contract monitor, CDC Project Officers, Public Health Advisors,

Surveillance Officers, Contracting Officer's Representatives, and others that may be determined in the future, that are responsible for accountability and oversight of the DDP project. The ISO must also submit a detailed written "initial report" within seven calendar days and a "final report" within 30 days of the initial report.

The Privacy Team and Security Teams will collaborate and confirm receipt of the breach notification, and perform a breach assessment to determine if the incident is, in fact, a breach.

The breach assessment involves:

- Gathering further details needed about the reported breach;
- Evaluating if a HIPAA exception applies;
- Identifying the safeguards in place at the time of the breach;
- Determining who had unauthorized access to the PHI;
- Identifying the specific information that was disclosed;
- Identifying whose privacy may have been breached;
- Assessing the possibility as to whether the PHI will be further disclosed;
- Determining if any sanctions are to be recommended upon staff contributing to the non-compliance;
- Reviewing and approving the Patient Notification Letter, which is required to be sent to the compromised individual(s) no later than 60 days from the date of breach;
- Working with the work unit to mitigate future breach incidents
- If subsequent information related to the breach is discovered after the initial breach report has been submitted to DHHS OCR, then the Privacy Team will submit an addendum to the initial DHHS OCR Breach Notification.

# Appendix

## Attachment 1. DDP Generic Fax Template

Virginia Department of Health

**Division of Disease Prevention**

P.O. Box 2448
Richmond, Virginia 23219
Physical Address: 109 Governor St, 3rd floor, Richmond, Virginia 23219
Main Office Number: 804-864-7000 Main Office Fax Number: 804-864-7970

# FACSIMILE

DATE: ___________________________________________________________________________

TO: ____________________________________________________________________________

FAX NUMBER: _____________________________________________________________________

PAGES (including cover sheet): _______________________________________________________

FROM: __________________________________________________________________________

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

Comments:

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

## Attachment 2. DDP Mailing Policy

### Policy for Mailing Confidential Patient Information

### Virginia Department of Health

### Division of Disease Prevention (DDP)

VDH VIRGINIA DEPARTMENT OF HEALTH
*To protect the health and promote the well-being of all people in Virginia.*

**DDP** programmatic forms (**HIV Counseling, Testing, and Referral [CTR} Forms, Interview Records, Field Records, and Epi-1s)** containing confidential patient information may be sent and received via a secure mail system, provided the mailing is done in a confidential manner that meets or exceeds the following:

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

- Forms shall be placed inside the "first" envelope and securely sealed. This envelope shall be marked "confidential". The envelope must protect contents from being read or viewed, and a regular manila envelope will meet this requirement. The number and type of forms being sent shall be indicated on the outside of the inner envelope.
- The "second" or outer envelope must be made of a material that is tear-, puncture-, and moisture-resistant, such as Tyvek. DDP will provide these envelopes for use by HIV testing sites and staff performing disease intervention activities.

- The recipient and sender name and address shall be placed on both envelopes. United Parcel Service (UPS) mailing labels for "return service" will be sent to local health districts and HIV testing sites. The UPS label shall be placed on the "second" or outer envelope. Double addressing gives an additional level of security that the package will reach the intended person/address.
- Mail shall be marked *"Confidential, To Be Opened By Addressee Only."*

- The frequency of mailing shall be at least weekly; this will avoid the risk of overstuffed envelopes which could be damaged in transit. It is suggested that mailings be combined where activities are occurring in multiple clinics at the same location if the volume is typically low. If UPS service has not been established, a call for pick-up will be necessary.

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

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

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

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

Your signature below indicates that:

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

**Name *(print)*:__________________________Signature:_________________________________Date:_____________**

**Supervisor's Signature: ________________________________________ Date: ___________________**

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

________________________________

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