DC | HEALTH
GOVERNMENT OF THE DISTRICT OF COLUMBIA

<table>
<tr><td colspan="2">District of Columbia Department of Health Ryan White HIV/AIDS Program Policies and Procedures

<b>External Data Security and Confidentiality</b></td><td><b>Policies and Procedures</b>
Implementing Office: HAHSTA Care and Treatment Division Ryan White HIV/AIDS Program (RWHAP)

Originally Issued: October 20, 2025

Revised: N/A</td></tr>
<tr><td><b>Program Approval:</b>

__ ______
Ebony Fortune
Deputy Chief, Care & Treatment</td><td><b>Recipient Authorization:</b>

____
Avemaria Smith
Ryan White Recipient</td><td><b>Effective Date:</b> December 9, 2025

<b>Valid Through Date:</b> December 9, 2026</td></tr>
<tr><td colspan="3"><b>I. SUBJECT</b>
External Data Security and Confidentiality</td></tr>
<tr><td colspan="3"><b>II. PURPOSE</b>
The purpose of this policy is to provide guidance on data security and confidentiality best practices for Ryan White subrecipients.</td></tr>
<tr><td><b>III. Definitions and Acronyms</b></td><td colspan="2"><b>Breach –</b> an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. For more details on the Privacy Rule, visit: Summary of the HIPAA Privacy Rule | HHS.gov

<b>CAREWare</b> – a free HRSA-mandated, web-based electronic health and social support services information system that captures client level data for HRSA's Ryan White HIV/AIDS Program recipients and providers.

<b>Corrective Action Plan</b>- is a structured approach to identifying, addressing, and preventing recurring or urgent issues in an organization. The plan comprises detailed action steps that must be completed by subrecipients to address areas of noncompliance. CAP helps resolve problems at their root cause while improving processes and accountability.

<b>Data Sharing Agreement</b>- an agreement that provides the terms and conditions under which HAHSTA shall have access to certain confidential data gathered by subrecipients during the duration of the grant period

<b>Health Insurance Portability and Accountability Act (HIPAA)</b> – a federal law enacted in 1966 to provide individuals with rights regarding the portability and renewability of their health insurance coverage, and to standardize and secure the electronic exchange of health information. For full details on HIPAA, visit: <i>The Health Insurance Portability and Accountability Act of 1996.</i></td></tr>
</table>

Personally Identifiable Information (PII) – refers to a broad classification of information that can be used to identify, contact, or locate a single person, either directly or when combined with other information. Examples of PII include:

- **Name**
- **Social Security Number**
- **Date and Place of Birth**
- **Mother’s Maiden Name**
- **Biometric Records**
- **Date of Birth**
- **Zip Code**

Protected Health Information (PHI) – refers to any health-related information about an individual’s health, treatment, and payment information, and any further information maintained in the same designated record set that could identify the individual or be used with other information in the record set to identify the individual. PHI is a subset of PII and is protected under HIPAA. Examples of PHI include:

- **Name**
- **Mailing address**
- **Email address**
- **Date and place of birth**
- **Telephone and fax numbers**
- **Social security number**
- **Mother ‘s maiden name**
- **Hospital admission and discharge date**
- **Date of death**
- **Dates of Service**
- **Health plan numbers**
- **Health records, health histories, lab test results, and medical bills**
- **License numbers**
- **Medical, educational, financial, and employment information**
- **Full face photographic images**
- **Biometric records (DNA, fingerprint, retina patterns)**

Protocol - a format for transmitting data between two computer devices. The protocol usually includes determination as to how the sending device will indicate that it has finished sending a message and how the receiving device will indicate that it has received the message.

Remediation Plan- a plan addressing performance issues that can be resolved through technical assistance

ShareFile - the secure web-based application used to share files and sync software that supports all the document-centric tasks and workflow needs of the Ryan White program. It

	is the CARE and Treatment division's HIPAA compliant file sharing system used to exchange protected health information (PHI) between staff and subrecipients. **Virtual Private Network (VPN)**- a virtual network built on top of existing networks that can provide a secure communications mechanism for data and IP information transmitted between networks
IV. Procedures	HAHSTA and its sub-recipients must follow this standardized data security and confidentiality policies and procedures to ensure personally identifiable information (PII) and protected health information (PHI) is used for legitimate public health activities and are not intentionally or inadvertently released for unauthorized or unethical purposes. Maintaining the confidentiality and security of public health data is a priority across all Ryan White programs. Ryan White subrecipients shall use the following procedures to ensure compliance with Ryan White program expectations: **A. Data Security and Confidentiality Requirements** 1. Control and limit access to patient's data: • Avoid using or sharing same CAREWare credentials • Remove CAREWare account for users who leave your organizations within 15 days of departure 2. Method for sharing customers level data with HAHSTA: • Use ShareFile to exchange customer data with HAHSTA • Do not share customer demographic or clinical information through emails or text messages • Subrecipients are required to enter into Data Sharing Agreements with HAHSTA, and have signed agreement(s) on file within 30 days from the beginning of the grant year **B. Working Remotely** • Avoid public Wi-Fi and use encrypted web connections • Restrict data to organization-issued computers/devices • Block sight lines when working in public spaces • Never leave devices unattended • Keep operating system and software up to date • Use virtual private network (VPN), when available **C. Reporting Ryan White Data Breaches and Repercussions** All data breaches involving PHI and PII must be reported to HAHSTA by subrecipients using the reporting procedures outlined below.

I. Reporting Data Breaches

In the event of a security breach incident, timely and clear communication is essential. Subrecipients must adhere to the following:

1. Identify the PHI or PHI that was breached.
2. Report cybersecurity-related issues, activities, or concerns related to Ryan White programs and systems, including CAREWare, to the Ryan White Data Team by emailing the Ryan White Program Data Team at care.ware@dc.gov and copying their immediate reporting supervisor.
    - Emails must include a copy to the assigned Ryan White Program Officer
    - Emails must be sent **within twenty-four hours** after discovering the incident and must describe as many details of the incident as possible. Do not forward any emails containing the data breach. The email reporting the breach must include the following:
        - Name of any entities, parties, agencies, and/or staff involved
        - Time and date of the incident
        - Source of the incident (email, text message, hard-copy document, invoice, etc.)
        - Description of incident/s, including but limited to sharing who the information was shared with and the agency's internal plan of action to resolve the issue

HAHSTA shall issue the following repercussions in the event there is a data security and/ or confidentiality breach to ensure the quickest resolution to regain compliance with any violated privacy laws and regulations, and to protect all parties involved:

II. Repercussions

1. **Subrecipients shall be notified of immediate rejection of invoice/progress report.** Upon identification of a data security breach or compliance violation, the subrecipient will be formally notified by HAHSTA that any pending invoice or progress report submission associated with the incident will be immediately rejected until the matter is addressed to HAHSTA's satisfaction.
2. **Subrecipients shall remove all unlawful documents**. Any documents found to be in violation of data privacy laws, federal regulations, or contract terms must be immediately removed from all records and systems. This includes, but is not limited to, documents containing personally identifiable information (PII), protected health information (PHI), or any data shared or stored without proper authorization.
3. **Subrecipients shall be required to submit a Remediation Plan after the 1st Offense.** For a first-time breach, the subrecipient will be required to submit a detailed remediation plan. This plan must outline the cause of the

	breach, immediate actions taken to contain it, and proposed steps to prevent recurrence. The plan must be approved by HAHSTA. 4. **Subrecipients are required to submit a Corrective Action Plan after the 2nd Offense.** A second breach will trigger the requirement for the subrecipient to submit a formal corrective action plan (CAP). The CAP must include a description of the root cause, a timeline for corrective measures, designation of responsible staff, and measurable outcomes. The plan must be approved by HAHSTA. Timely and satisfactory implementation of the CAP may directly or indirectly impact future funding. **5.** **Subrecipients may incur fines and/or possible termination of funding.** Repeated or severe violations may result in financial penalties, including cost disallowances. In cases of egregious noncompliance or failure to take corrective action, fines like those imposed under the *Data-Sharing and Information Coordination Amendment Act of 2010* may be invoked. Additionally, funding may be suspended or permanently terminated, in accordance with federal grant regulations and contractual agreements.
VI. Key Contacts	Ebony Fortune, Ryan White HIV/AIDS Program Manager, 202.671.4900 or Ebony.Fortune@dc.gov
VII. Related Documents, Forms, Resources and Tools	HIPAA Privacy Rule Health Insurance Portability and Accountability Act of 1996 Data-Sharing and Information Coordination Amendment Act of 2010 Guide to SSL VPNs: Recommendations of the National Institute of Standards and Technology Computer Security Resource Center Program Templates - Ryan White Data Sharing Agreement