

# VIIS REGISTRATION PROCEDURES

## STEP 1: ASSIGN AN ADMINISTRATOR

- The assigned administrator would be the main person for contact with VDH.
- VDH will activate the administrator into the system, who in turn will,
- Using a simple procedure, activate all of their organization's users
- Additional responsibilities include:
  - Establishing security roles for users within their own organization
  - Conducting/enforcing VIIS system security procedures
  - Maintaining VIIS user registration documentation on behalf of the organization

## STEP 2: ASSIGNED ADMINISTRATOR MUST FILL OUT THE FOLLOWING FIVE FORMS

- Organization Forms (2): Please complete one of the following per site you want registered
  - VIIS Organization/Vendor Registration Form
- Administrator User Forms (3):
  - VDH Information Systems Security Access Agreement Vendor Agreement
  - VIIS User Registration Form
  - VIIS Security Policy & User Confidentiality Agreement
  - VDH Information Systems Security Access Agreement (ISSAA)
    - **Each administrator must sign a copy of the ISSAA form**

## STEP 3: MAIL OR FAX COMPLETED FORMS:

### **Mailing Address:**

VIIS Support Staff or your VIIS Consultant  
Virginia Department of Health  
Division of Immunization  
109 Governor St. Rm 314 W  
Richmond, VA 23219

### **Fax:**

(804) 864-8190  
ATTN: VIIS Support Staff or your VIIS Consultant

## STEP 4: YEARLY UPDATE

Be sure to update your information yearly by filling out the "VIIS User Contact Information Update" form located under "Forms" at <https://www.viis.virginia.gov>

Commonwealth of Virginia  
Department of Health

Information Systems Security Access Agreement  
Vendor Agreement

As a user of the Virginia Department of Health (VDH) information systems, it is understood and agreed, to abide by VDH Security Policy and the following terms, which govern access to and use of, the information and computer services of VDH.

Access is being granted by VDH as a necessary privilege in order to perform authorized service functions for VDH. Passwords and logon IDs should not be shared. It is prohibited to use or knowingly permit use of any assigned or entrusted access control mechanisms (such as Logon IDs, passwords, terminal IDs or file protection) for any purposes other than those required to perform authorized service functions. It is agreed that passwords will be changed immediately if they are compromised and notification will be sent to the Office of Information Management (OIM). No passwords will be incorporated into any sign-on software.

If, due to authorized job functions, access is required to information on VDH information systems, which is not owned by the contracting division, written authorization for access to that information must be obtained from the information owner and presented to OIM.

It is agreed to not disclose any confidential, restricted or sensitive data to unauthorized persons. It is agreed to not disclose information concerning any access control mechanism of which we have knowledge unless properly authorized to do so, and we will not use access mechanisms, which have not been expressly assigned. VDH systems will not be used for commercial or partisan political purposes, such as using electronic mail to circulate advertising for products or for political candidates or issues.

We agree to abide by all applicable Federal and Commonwealth of Virginia Laws, and VDH agency policies, procedures and standards that relate to the security of VDH information systems and the data contained therein.

If incidents of non-compliance with the terms of this agreement are observed, we are responsible for immediately reporting them to the information Security Officer and management of VDH.

Consent is given to the monitoring of all activities on VDH information systems, and any other systems accessed through VDH systems.

By signing this agreement, it is hereby certified that we (the contracting vendor) understand the preceding terms and provisions and that we accept the responsibility of adhering to the same. We further acknowledge that any infractions of this agreement can and will result in actions being taken according to Federal and State Laws governing Information Systems Protection, including but not limited to the termination of access privileges and or criminal prosecution.

\_\_\_\_\_  
Organization Name (Print)

\_\_\_\_\_  
Division Name (Print, if applicable)

\_\_\_\_\_  
Signature of Administrator

\_\_\_\_\_  
Name of Administrator (Print)

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature of Administrator

\_\_\_\_\_  
Name of Administrator (Print)

\_\_\_\_\_  
Date

**Virginia Immunization Information System (VIIS)  
 Organization/Vendor Registration Form  
 (Required for Registering New Organization)  
 Organization/Vendor Information**

**1. Organization Type** – choose the appropriate entity from this list:

- |  |  |
|--|--|
| <input type="checkbox"/> Community Health Center / Rural Health Center | <input type="checkbox"/> Immunization Registry |
| <input type="checkbox"/> Child Care / Head Start Program               | <input type="checkbox"/> Military              |
| <input type="checkbox"/> College/University                            | <input type="checkbox"/> Pediatric Practice    |
| <input type="checkbox"/> Family Practice                               | <input type="checkbox"/> Private Clinic        |
| <input type="checkbox"/> Health Plan/Medicaid                          | <input type="checkbox"/> Private School        |
| <input type="checkbox"/> Health Plan/Non-Medicaid                      | <input type="checkbox"/> Public Health         |
| <input type="checkbox"/> Hospital                                      | <input type="checkbox"/> Public School         |
| <input type="checkbox"/> Mobile Health Care Clinic                     | <input type="checkbox"/> State                 |
| <input type="checkbox"/> Other Organization: Please Specify _____      |  |

**2. Organization/Site Name:**

\_\_\_\_\_

**3. Organization/Site Address:**

\_\_\_\_\_

*Street Address*

\_\_\_\_\_

*City, State and ZIP Code*

**Organization/Vendor Contacts**

**4. VIIS Administrator(s) for Organization/Vendor:**

Printed Name, Title	Signature	Date
---------------------	-----------	------

Printed Name, Title	Signature	Date
---------------------	-----------	------

**5. Phone:** (\_\_\_\_) \_\_\_\_\_  
**Alternate Phone:** (\_\_\_\_) \_\_\_\_\_

**6. Fax:** (\_\_\_\_) \_\_\_\_\_

**7. Email:** \_\_\_\_\_

**8. Are you a VFC Provider?** (Please check one) **YES** \_\_\_\_\_ **If Yes, Pin #:** \_\_\_\_\_  
**NO** \_\_\_\_\_

**9. Organization/Vendor Approval (optional):**

Printed Name, Title	Signature	Date
---------------------	-----------	------

**10. For Children Organizations, specify Parent Organization Name\*:** \_\_\_\_\_

**\* VIIS has a parent/child hierarchy. Parent = Main Site; Child = Satellite Sites**

11. Please fill out the following information for all requested users.

	Last Name	First Name	Middle Name/ Initial	Professional Title	VIIS Security Role*
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					

**VIIS Role Types:** **RO=Reports Only** (View VIIS/Run Reports, NO Data Entry), **T=Typical User** (Enters Patient and Immunization Data, Runs Reports, NO Inventory Control), **IC=Inventory Control** (Enters Inventory, Patient, and Immunization Data, Runs Reports), **DE=Data Exchange** (Submits/Receives Files via VIIS Data Exchange Process/HMO) or **A=Administrator** (VIIS Organization/Site Administrator, sets up user accounts, views all modules) **TUR=Typical User and Reports** – Allows Typical User to run ALL reports and not just Client-Specific Reports.



# VIIS Security Policy & User Confidentiality Agreement

## **VIIS Information:**

*The Code of Virginia, § 32.1-46.01 authorizes the Virginia Immunization Information System (VIIS), a statewide immunization information system that manages electronic immunization records. This policy states behaviors required of VIIS users, Virginia Department of Health (VDH), and Division of Immunization (DOI) to protect the confidentiality, privacy and accuracy of client information.*

1. VIIS is consistent with the Department of Health and Human Services and the Health Insurance Portability and Accountability Act (HIPAA) of 1996.
2. Authorized users of VIIS will include:
  - a. Health care provider or health plans
  - b. Schools or other organizations that provide health care services
  - c. Individuals or organizations as required by law or in the management of a public health crisis
  - d. Other immunization registries
3. The review of this policy must involve the participation of representatives from the private and public health care sectors.

## **VDH/DOI Host Site Security:**

1. The system will force users to change their password every 30 days.
2. The VIIS system will time-out after 45 minutes.
3. No information from VIIS will be made available to law enforcement, the Immigration and Naturalization Service, or any other party.
4. The VIIS system will maintain an audit trail for all information accessed.
5. VDH/ EDS will conduct a self-assessment of the potential risks and areas of vulnerability regarding VIIS and will develop, implement, and maintain appropriate security measures on an ongoing basis.
6. The release of immunization information shall be for statistical purposes or for studies that do not identify individuals.

## **Provider/ User Security:**

1. Access to VIIS information is authorized under the condition that it is required to perform my job function
2. All VIIS users will be required to sign a Confidentiality/ Security Agreement with VDH
3. Each user must renew the user confidentiality/security agreement every two years.
4. Each user is responsible for maintaining confidentiality.
5. The user has the obligation to act on any request by an individual to opt out of VIIS. If the patient elects to opt out, the provider should promptly mark the record in VIIS as “Do Not Share”, so that only that provider may view the client’s immunization records
6. The user will make reasonable effort to ensure the accuracy of all immunization and demographic information entered or edited
7. Virus protection is recommended for each client site.
8. User desktops/laptops must have physical security and password screen savers when not being used by authorized individuals.
9. Users will terminate the VIIS application prior to leaving the VIIS workstation
10. An ID and Password are required to access VIIS.
11. Users will not share or disclose their ID or password to anyone.
12. VIIS records will be treated with the same vigilance, confidentiality, and privacy as any other patient medical record.

13. Patient immunization records will not be copied except for authorized use
14. VIIS information in a paper copy will not be left where it would be visible for unauthorized personnel and must be shredded before disposal
15. The VIIS Administrator will maintain completed user registration forms in a secure location
16. Unauthorized disclosure of information from confidential records may be punishable, upon conviction, by a fine and/or imprisonment or both, and/or civil penalties as prescribed by law as well as sanctions and/or disciplinary action.
17. If VIIS data is to be faxed, the sender must verify the fax number and receipt of data.
18. Any activity that would jeopardize the proper function/security of VIIS will not be conducted. Misuse of VIIS may result in legal action against me personally, and against the organization for which I am an agent

**Provider Responsibility:**

1. A copy of this agreement has been provided to me
2. The VIIS Administrator at the user site will terminate access for an authorized user who no longer requires access.
3. The VIIS Administrator will maintain completed user registration forms in a secure location
3. Users will make every effort to protect VIIS screens from unauthorized view.
4. Should a material breach of personal privacy/confidentiality occur, the offending party must immediately notify the client and VDH/ DOI designee. Violators of this policy will be restricted from VIIS by the System Administrator at the offender's site.
5. The VIIS Administrator will be notified immediately if unauthorized entry into the system is suspected.

**Approved by:**

To be signed by one representative that has the delegated authority to act on behalf of the User organization and one representative that has the delegated authority to act on behalf of VDH/DOI.

\_\_\_\_\_  
User Company/Organization Name (Print)

*Administrator*

\_\_\_\_\_  
Name of VIIS User (Print)

\_\_\_\_\_  
Signature of VIIS User

\_\_\_\_\_  
Title

\_\_\_\_\_  
Date

*Administrator 2 (if applicable)*

\_\_\_\_\_  
Name of VIIS User (Print)

\_\_\_\_\_  
Signature of VIIS User

\_\_\_\_\_  
Title

\_\_\_\_\_  
Date

Reviewed on 11-02-2007



Commonwealth of Virginia  
Department of Health  
Information Systems Security Access Agreement

As a user of the Department of Health (VDH) information systems, I understand and agree to abide by VDH Security Policy and the following terms which govern my access to and use of the information and computer services of VDH.

Access has been granted to me by VDH as a necessary privilege in order to perform my authorized job functions for VDH. Passwords and logon IDs should not be shared. I am prohibited from using or knowingly permitting use of any assigned or entrusted access control mechanisms (such as Logon IDs, passwords, terminal IDs or file protection) for any purposes other than those required to perform my authorized employment functions. I agree to change passwords immediately if they are compromised. I will not incorporate passwords into any sign on software.

If, due to my authorized job functions, I require access to information on VDH information systems which are not owned by my division, I must obtain authorized access to that information from the information owner and present access documentation to Data Administration (Office of Information Management).

I will not disclose any confidential, restricted or sensitive data to unauthorized persons. I will not disclose information concerning any access control mechanism of which I have knowledge unless properly authorized to do so, and I will not use access mechanisms which have not been expressly assigned to me. I will not use VDH systems for commercial or partisan political purposes, such as using electronic mail to circulate advertising for products or for political candidates or issues.

Having read the VDH Security Awareness Web site and corresponding sections on Personal Computer (PC) Use, Computer Access Security, and Data Security in the VDH Information Technology Resources Policy and Procedures Manual, I certify that I have received Computer Security Awareness training and understand my security responsibilities as a user of the Department of Health (VDH) information systems.

I agree to abide by all applicable Federal, Commonwealth of Virginia, and VDH agency policies, procedures and standards which relate to the security of VDH information systems and the data contained therein.

If I observe incidents of non-compliance with the terms of this agreement, I am responsible for reporting them to the information Security Officer and management of VDH.

I give consent to the monitoring of my activities on VDH information systems, and other systems accessed through VDH systems.

By signing this agreement, I hereby certify that I understand the preceding terms and provisions and that I accept the responsibility of adhering to the same. I further acknowledge that any infractions of this agreement will result in disciplinary action according to the State Employee Rules of Conduct, including but not limited to the termination of my access privileges.

\_\_\_\_\_  
Employee/Consultant Name (Print)

\_\_\_\_\_  
Date of Signature

\_\_\_\_\_  
Employee/Consultant Signature

\_\_\_\_\_  
Organization Name