

VIIS Security Policy And 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. VIIS is consistent with the Department of Health and Human Services and the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Authorized users of VIIS will include:

- Health care provider or health plans.
- Schools or other organizations that provide health care services.
- Individuals or organizations as required by law or in the management of a public health crisis.
- Other immunization registries.

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 30 minutes.
3. The VIIS system will maintain an audit trail for all information accessed.
4. VDH/HP 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.
5. The release of immunization information shall be for statistical purposes or for studies that do not identify individuals.
6. VDH/DOI will work with interested data exchange partners through Data Exchange steps outlined in MOA.

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 year.
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 a 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. Participants in data exchange shall provide an acceptable level of data quality, such as correct data fields, data accuracy and enough information to correctly merge with existing clients. Upon initial data delivery, and periodically thereafter, data shall be reviewed to determine data quality. Any rejected records shall be resolved by the participant in a timely way. VDH may suspend system privileges and refer to Virginia Code § 32.1-27 for additional action for any organization that submits inaccurate data.
14. Any inappropriate use of VIIS data shall result in immediate suspension of user privileges and result in an investigation conducted by VDH. Additional actions may be taken in accordance with Virginia Code § 32.1-27. The VIIS program manager may reinstate privileges upon satisfactory completion of required remedial actions and guarantee of proper use of VIIS in the future.

I read and agree to the security policy.

Administrator Policy:

As VIIS administrator, it is my responsibility to ensure my VIIS users :

- are actively employed at my organization.
- need access to VIIS for his or her job.
- have been assigned the correct role in VIIS.
- and have reviewed and agreed to the VIIS Security and Confidentiality policy.

I certify all user accounts in VIIS are in accordance with the above statement.