

## **ATTACHMENT D**

### **PARTICIPATING ORGANIZATION SECURITY REQUIREMENTS**

In addition to any obligations set forth in the Participant Agreement and the WVHIN Policies and Procedures, the PO shall observe the following requirements. The WVHIN may amend or supplement these requirements on written notice to PO issued in accordance with Section 2(d) of the Terms and Conditions contained in Attachment B.

1. Each of the PO's servers connecting to the WVHIN gateway or portal shall comply with the WVHIN's authentication requirements, implementing Encryption technology and certificates issued or approved by WVHIN.

2. The PO shall comply with the WVHIN Interoperability Guide when connecting to the Health Information Exchange.

3. The PO will authenticate each Authorized User at the point of access, and shall implement Authentication Information based on the WVHIN's Policies and Procedures. The PO shall review and update its list of Authorized Users as required under Attachment A and the WVHIN Policies and Procedures.

4. The PO shall limit access of each Authorized User to his or her Permissible Purposes and according to the role based access principles implemented by the PO. The PO shall impose appropriate sanctions for members of its Workforce who violate the WVHIN's Policies and Procedures, violate the Authorized User Agreement, or make improper use of the Health Information Exchange, including revocation of an Authorized User's access the Exchange as may be appropriate under the circumstances.

5. The PO shall maintain access logs that capture user identification information associated with the PO's system.

6. The PO shall implement message-level security using Encryption technology acceptable to the WVHIN.

7. The PO shall implement commercially robust firewalls and intrusion detection methods acceptable to the WVHIN. The PO shall also perform periodic automated and random manual review and verification of audit logs for both operational monitoring and system security as required by the WVHIN's Policies and Procedures.

8. The PO shall implement other safeguards to ensure that its connection to and use of the Health Information Exchange, including without limitation the medium containing any Protected Health Information or other information provided to the Exchange, does not include and shall not introduce any program, routine, subroutine, or data (including without limitation malicious software, malware, viruses, worms, or Trojan horses) which will disrupt the proper operation of the Exchange or any part thereof, or upon the occurrence of an event, passage of time, or taking or failure to take any action, shall cause the Exchange or any other PO to be destroyed, damaged, or rendered inoperable.

9. The PO shall undertake a full, accurate, and thorough risk analysis to identify its own system's security vulnerabilities in order to determine reasonable and appropriate safeguards to ensure the confidentiality, security, and integrity of Protected Health Information held by the PO.

10. The PO shall implement and maintain appropriate safeguards to ensure the confidentiality, security, and integrity of Protected Heal Information held by the PO in full compliance with the HIPAA Security Rules.