ATTACHMENT D
PARTICIPATING ORGANIZATION/SUBSCRIBER SECURITY REQUIREMENTS

In addition to any obligations set forth in the Participant Agreement, the Subscription Agreement, and the WVHIN Policies and Procedures, the PO or Subscriber (collectively referred to herein as the "PO/S") shall observe the following requirements. The WVHIN may amend or supplement these requirements on written notice to PO/S issued in accordance with Section 2(d) of the Terms and Conditions contained in Attachment A1 or A2, or to a Subscriber upon 30 days' notice.

1. Each of the PO/S'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/S shall comply with the CRISP connectivity guidelines when connecting to the Health Information Exchange.

3. The PO/S 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/S shall review and update its list of Authorized Users as required under Attachment A1 or A2, as applicable, and the WVHIN Policies and Procedures.

4. The PO/S shall limit access of each Authorized User to his or her Permissible Purposes. The PO/S shall impose appropriate sanctions for members of its Workforce who violate the WVHIN's Policies and Procedures, or make improper use of the Health Information Exchange, WVDirect, or the WV e-Directive Registry (collectively, the "WVHIN's Systems"), including revocation of an Authorized User's access to the WVHIN's Systems as may be appropriate under the circumstances.

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

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

7. The PO/S shall implement commercially robust firewalls and intrusion detection methods acceptable to the WVHIN. The PO/S 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/S shall implement other safeguards to ensure that its connection to and use of the WVHIN's Systems, including without limitation the medium containing any PHI or other information provided to the WVHIN's Systems, 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 WVHIN's Systems, or upon the occurrence of an event, passage

of time, or taking or failure to take any action, shall cause the WVHIN's Systems to be destroyed, damaged, or rendered inoperable.

9. The PO/S 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 PHI held by the PO/S. The PO/S shall develop and implement policies, procedures, and staff training as required by HIPAA Security Rules.

10. The PO/S shall implement and maintain appropriate safeguards to ensure the confidentiality, security, and integrity of PHI held by the PO/S in full compliance with the HIPAA Security Rules. Because files containing PHI may be stored on the PO/S's system, computers should be protected (i.e., whole disk encryption, not left unattended or unlocked, etc.). It is also important to lockdown and encrypt your wireless network.

11. Authorized Users of the PO/S should not access WVHIN's Systems from non-secure devices such as public use workstations, home computers, or other similarly non-secure devices, or through unsecured networks or wireless hotspots where technical and physical security cannot be controlled.

12. Accessing the WVHIN's Systems from the mobile devices (laptops, smartphones, tablets, etc.) of Authorized Users is not prohibited; however, devices must be secured. Each PO/S and its Authorized Users should examine the benefits and risks associated with accessing and potentially storing PHI located on mobile devices. The following protection mechanisms should be implemented to protect any PHI shared through the WVHIN's Systems that is stored locally on a mobile device:

- Device password lock activated and used to gain local access to the given device,
- Virus and other malware protection,
- File encryption and/or encryption of data at rest, and
- Remote wipe enabled in case of device loss.

It is also strongly recommended that PO/S's include the following protection mechanisms for all devices used by their affiliated users:

- Establishing PHI deletion policies and media disposal procedures for mobile devices,
- Maintaining an accurate mobile device tracking and asset management program,
- Developing policies for the proper use or restriction of personal mobile devices for access to any of the WVHIN's Systems.

13. Each WVDirect subscriber must ensure that secure communications involving patient data are with other Direct subscribers. Any Patient authorization or consent required by applicable law for the disclosure of Sensitive Health Information (for example, in the case of Drug or Alcohol Abuse Information) must be obtained prior to the disclosure of such Sensitive Health Information through the use of WVDirect.