Attachment A5
WV e-Directive Registry Agreement
Health Care Provider Registration

This form is used by health care providers to register for access to the repository of advance directives maintained by the WV e-Directive Registry and made available on-line by the WVHIN. The identity of all participants will be validated by a representative of the WVHIN or the Participating Organization's Authorized Administrator. Complete this Agreement and return it to the WVHIN or its representative to request your organization's access to the e-Directive Registry.

Member Organization Information:

Organization Name	
Address 1	
Address 2	
City	
County	
State	
Zip Code	
Phone Number	
E-Mail Address	
Group NPI Number	
Fax Number (asso w/NPI)	
Point of Contact Name	
Business Web Address	

Facility Type: (check one)

Hospital: □ General Acute □ Critical Access □ Rehabilitation □ Psychiatric □ Long Term Care

□ Primary Care Provider □ Specialist □ FQHC □ Local Health Department □ Lab

□ Pharmacy □ Urgent Care □ Ambulatory Surgery □ Behavioral Health □ Long Term Care

□ Home Health □ Hospice □ Other _____

Terms and Conditions

By signing this Agreement, Health Care Provider, its officers, directors and employees agree to the following terms and conditions:

1. All information provided on this form is true and accurate as of the date of execution. Business and professional licenses must be kept current in order to remain an e-Directive enrollee.

2. If any of the information above changes, the WVHIN will be notified as soon as possible by e-mail to _____ or by phone 304-558-4503.

3. A separate WV e-Directive Registry account maintained by your organization must be established for each individual employee requiring access. WV e-Directive accounts may only be established for individual employees of your organization authorized to access, use, or transmit PHI in order to perform their job duties.

4. Access to the WV e-Directive Registry established at the individual employee level must be tightly controlled and monitored. Your organization must identify the individual employees designated with access to the WV e-Directive Registry.

5. Each individual employee for whom a WV e-Directive Registry account is established shall be responsible for all activities associated with the account assigned to him or her.

6. Your organization must delete access to WV e-Directive Registry accounts established for individual employees no longer employed by your organization within one business day of the employee's last day at your organization. If an employee is terminated due to less than favorable circumstances, access to the account must be deleted immediately.

7. A WV e-Directive Registry account is to be used by a designated individual employee to access and confirm a Patient's desires for end-of-life care, including advance directive forms, Physicians Orders for Scope of Treatment (POST) forms, and do not resuscitate cards.

8. Your organization will encourage best practices for patient privacy protections related to the use of each WV e-Directive Registry account established for individual employees of your organization. In doing so, your organization will vigorously enforce the Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH") Privacy and Security Rules, including, with limitation, maintaining the confidentiality

and security of PHI; implementation of administrative, technical, and physical safeguards to prevent unauthorized access, use and transmission of PHI; only access, use, or disclose PHI as authorized by the patient in a treatment relationship; mitigate any risks associated with an unauthorized access, use or disclosure of PHI; require any subcontractors that receive, use or have access to PHI to comply with the Privacy and Security Rules; and disclose only the minimum PHI necessary for the purpose for which it is disclosed.

9. In accordance with WVHIN Policies, your organization will promptly notify WVHIN if there is a breach, as defined under either state or federal law, that may in any way affect your WV e-Directive Registry account.

10. If an individual Opts-Out of the WVHIN's Health Information Exchange, no PHI pertaining to that individual may be shared via the Health Information Exchange. This includes information contained in the WV e-Directive Registry.

11. Your organization will execute a BAA with the WVHIN. (Attachment B)

12. The WVHIN reserves the right to deny or remove access to the WV e-Directive Registry for any violation of the terms of this Agreement.

I hereby certify that my organization provides healthcare services to WV patients and I am authorized to act on behalf of the organization to participate in the WV e-Directive Registry, to sign this Agreement and that the information contained herein is true and accurate.

Organization Name	WVHIN Representative Signature
Corporate Officer Signature	Notary Public Signature Note: A notary is not required is the signature has been verified by a WVHIN Representative
Print Corporate Officer Name	
Title Date	

Authorized Administrator Information

The Authorized Administrator is appointed to communicate with WVHIN and act on behalf of your organization with respect to all aspects of the WV e-Directive Registry. The Authorized Administrator is also responsible for maintaining the organization's individual WV e-Directive accounts, and for deleting those accounts in a timely manner consistent with this Agreement. The Authorized Administrator must provide valid government issued identification such as a current driver's license or passport in order to verify their identity.

Administrator Name	
Title	
Role	____Physician ____NP/RN/MA ____Administrator ____Other _____
Govt Issued ID #	

Signature of Authorized Administrator: _____
Identity of Authorized Administrator verified by:

WVHIN Representative Signature _____

_____
Notary Public Signature (Note: A notary is not required if the signature has been verified by a WVHIN Representative)

Attachment A

West Virginia Health Information Exchange (WVHIN)
WV e-Directive Registry Security Best Practices

The following provide best practices on user-controlled activities related to the use of the WV e-Directive Registry service. These practices do not, in and of themselves, determine whether a WV e-Directive user is fully compliant with HIPAA Security and Privacy requirements as defined in "Security Standards for the Protection of Electronic Protected Health Information (EPHI)" (45 CFR Part 164, Subpart C), commonly known as the Security Rule, and in "Privacy of Individually Identifiable Health Information" (45 CFR Part 164, Subpart E), commonly known as the Privacy Rule.

Keep your computer secure:
When using the WV e-Directive Registry, it is important to follow the same security guidelines currently used at your practice for computers containing PHI. Because files containing PHI might need to be stored in your computer, it is important that the computer is protected (i.e., whole-disk encryption, not left unattended and unlocked, etc.). It is also important to lockdown and encrypt your wireless network.

Download PHI from your WV e-Directive Account only to a secured workstation computer:
The WV e-Directive Registry should not to be accessed from non-secure devices such as public use workstations or home computers where security controls cannot be enforced. Public use workstations and other non-secure devices are those where general public access is allowed, or where security technical and physical security requirements cannot be applied and controlled. You should only download information from the WV e-Directive Registry to a secured computer.

Accessing WV e-Directive Registry via Mobile Devices
Accessing the WV e-Directive Registry from mobile devices (laptops, smartphones, tablets, etc.) is not prohibited; however, each WV e-Directive subscriber organization and individual user should examine the risk associated with potentially having PHI located on these devices through the sharing of patient data. The following protection mechanisms should be implemented to protect any PHI shared through the WV e-Directive Registry that is stored locally on a user device:

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

It is also strongly recommended that subscribing organizations include, but not be limited to, 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 PHI system.
-

Email Confidentiality Notices

Each WV e-Directive Registry subscriber has a responsibility to ensure the protection of patient data that is viewed or discussed through the Registry consistent with the HIPAA Privacy Rule, including disclosures to unauthorized individuals. Each WV e-Directive Registry user must ensure that communications involving patient data are between authorized individuals and that any authorizations or consents required by applicable law are obtained prior to disclosure.