WEST VIRGINIA
SECRETARY OF STATE
NATALIE E. TENNANT
ADMINISTRATIVE LAW DIVISION

Do Not Mark In This Box

FILED

2014 APR 18 A 9:41

OFFICE WEST VIRGINIA SECRETARY OF STATE

Form #6

NOTICE OF FINAL FILING AND ADOPTION OF A LEGISLATIVE RULE AUTHORIZED BY THE WEST VIRGINIA LEGISLATURE

AGENCY: West Virginia Health Care Authority/West Virginia Health Information Network TITLE NUMBER: 65

AMENDMENT TO AN EXISTING RULE: YES X NO ____

IF YES, SERIES NUMBER OF RULE BEING AMENDED: 28

TITLE OF RULE BEING AMENDED: West Virginia Health Information Network Rule

IF NO, SERIES NUMBER OF RULE BEING PROPOSED: ____

TITLE OF RULE BEING PROPOSED: ____

THE ABOVE RULE HAS BEEN AUTHORIZED BY THE WEST VIRGINIA LEGISLATURE.

AUTHORIZATION IS CITED IN (house or senate bill number) SB 155.

SECTION §64-5-3, PASSED ON March 8, 2014

THIS RULE IS FILED WITH THE SECRETARY OF STATE. THIS RULE BECOMES EFFECTIVE ON THE FOLLOWING DATE: May 18, 2014

Authorized Signature

TITLE 65
LEGISLATIVE RULE
HEALTH CARE AUTHORITY

SERIES 28
WEST VIRGINIA HEALTH INFORMATION NETWORK RULE

§65-28-1. General.

1.1. Scope – This legislative rule establishes the standards for the development, implementation, and operation of the West Virginia Health Information Network (Network) as an interoperable statewide network for health information exchange.

1.2. Authority – W.Va. Code §§16-29G-7 and 16-29B-8(a) (1).

1.3. Filing Date – April 18, 2014.

1.4. Effective Date – May 18, 2014.

1.5. Construction – This legislative rule shall be liberally construed to comply with any and all applicable federal and state laws designed to ensure the privacy and security of health information.

§65-28-2. Definitions.

2.1. Authentication Information – means the method of authentication assigned to each authorized user of the Network by his or her participating organization in accordance with minimum Network requirements. Authentication Information may be based upon information known only by and unique to an authorized user, such as a password and username. The Network may impose a second authentication factor that is based upon something that an authorized user has, such as a smart card or token, or something unique to the authorized user, such as an electronic signature or fingerprint.

2.2. Authorized User – means a member of the workforce of a participating organization who has been designated by that participating organization to access the Network's health information exchange pursuant to the concept of role-based access control. An authorized user may also be a patient who has registered for access to the Network's patient portal to obtain direct access to his or her protected health information from a cooperating participating organization; a member of the Network's workforce; or a member of the workforce of a business associate of the Network.

2.3. Business Associate – means a person or entity that performs a function, activity, or service to a health care provider, health plan, health care clearinghouse, or another business associate involving the disclosure of protected health information or personal demographic information to the business associate. The Network is a business associate to each of its participating organizations. Subcontractors and vendors to the Network may be business associates of the Network. The term "business associate" has the same meaning as the term is defined in 45 C.F.R. Part 160.

2.4. Business Associate Agreement – means a contract between a covered entity under HIPAA and a business associate, or between a pair of business associates, which obligates the business associate to maintain the privacy and security of protected health information in accordance with the requirements of 45 C.F.R. Part 164.

2.5. Breach – means the acquisition, access, use, or disclosure of a patient's unsecured protected health information by an unauthorized person or entity in a manner not permitted under the HIPAA privacy rules, and in a manner that otherwise satisfies all other requirements imposed by the rules governing breach notification for unsecured protected health information in 45 C.F.R. Part 164.

2.6. Clinical Messaging – means the exchange of protected health information from one participating organization to another through the Network in the form of test results or other clinical information. Test results can be generated by clinical laboratories, imaging providers, and other like providers. Other clinical information may consist of discharge summaries, consultation reports, and patient referral data. For purposes of the Network's health information exchange, clinical messaging is a point-to-point transaction.

2.7. Consent – means the decision of a patient to participate in the Network's health information exchange. No affirmative action is required from a patient to establish his or her consent. A patient shall be considered to have given his or her consent to participate until and unless the patient affirmatively opts-out of the health information exchange.

2.8. Covered Entity – means a health care provider, a practitioner licensed under the provisions of Chapter 30 of the West Virginia Code or some equivalent law of another state, a health care clearinghouse, or a health plan that transmits any protected health information in electronic form. The term "Covered Entity" has the same meaning as the term defined in 45 C.F.R. Part 160.

2.9. Data Supplier – means any organization approved by the Network that has entered into a data supplier agreement and discloses or otherwise makes available protected health information for access through the Network's health information exchange for a permissible purpose.

2.10. Data User – means a participant that has entered into a data user agreement and whose authorized users will access, receive, and use protected health information through the health information exchange for a permissible purpose. By entering into a data user agreement, participant may access and use the WV e-Directive Registry.

2.11. Deidentify or Deidentification – means the process of rendering protected health information into a form that does not identify a patient, and there is no reasonable basis to believe that the information can be used to identify a patient. In order to deidentify protected health information properly, the requirements of 45 C.F.R. Part 164 must be fully satisfied.

2.12. Designated Record Set – means any grouping of medical or billing records maintained by a covered entity and used to make treatment or payment decisions about a patient. A designated record set shall have the same meaning as the term is defined in 45 C.F.R. Part 164, Subpart E.

2.13. Drug or Alcohol Abuse Information – means information related to the treatment and care of a patient suffering from alcohol or drug abuse, or both, including any information that would specifically identify a patient as receiving drug or alcohol abuse treatment and care. The term "Drug or Alcohol Abuse Information" has the same meaning as the term "Drug or Alcohol Abuse Patient Records" is defined in 42 C.F.R. Part 2. Drug or alcohol abuse information, for purposes of this rule, shall arise only in connection with care and treatment provided in a federally assisted program as defined in 42 C.F.R. Part. 2.

2.14. Emergency Treatment – means a condition which poses an immediate threat to the health of a patient (for example, death or serious impairment to one or more bodily systems, organs, or parts), and which requires immediate medical intervention.

2.15. Encryption – means a technology or methodology approved by the United States Secretary of Health and Human Services that can render protected health information unusable, unreadable, or indecipherable to unauthorized individuals or entities.

2.16. E-Prescribing – means the transmission, using electronic media, of prescription or prescription-related information between a licensed practitioner and a pharmacy, pharmacy benefit manager, or health plan, including any communication related to the prescription.

2.17. Full Service Participant – means a participant that has entered into a full service agreement and that functions as both a data supplier and a data user within the health information exchange. By entering into a full service agreement, participant may access and use the WV e-Directive Registry.

2.18. Health Care Clearinghouse – means any entity, including a billing service, repricing company, or other similar organization that processes health information in a nonstandard format into standard data elements or a standard transaction, or vice versa. The term "Health Care Clearinghouse" has the same meaning as such term is defined in 45 C.F.R. Part 160.

2.19. Health Care Provider – means a provider of medical or health services, and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. The term "Health Care Provider" has the same meaning as the term is defined in 45 C.F.R. Part 160.

2.20. Health Plan – means an individual or group plan that provides, or pays the cost of medical or health services. The term "health plan" has the same meaning as such term is defined in 45 C.F.R. Part 160.

2.21. Health Care Operations – means any of those activities identified by federal regulations at 45 C.F.R. Part 164, including but not limited to, quality assessment and improvement activities, case management and care coordination, reviewing the competence of licensed practitioners, underwriting, and business planning and management activities.

2.22. Health Information Exchange – means a system for the electronic transfer of protected health information between participating organizations for a permissible purpose based upon requirements of federal and state law. A health information exchange shall seek to achieve interoperability between and among its participating organizations.

2.23. HIPAA – means the Health Insurance Portability and Accountability Act of 1996, and its implementing rules promulgated in 45 C.F.R. Parts 160, 162, and 164.

2.24. HIPAA Privacy Rules – means those privacy rules described in 45 C.F.R. Part 164, Subpart E, as modified and enlarged by the Health Information Technology for Economic and Clinical Health (HITECH) Act and any other subsequent amendments as of the effective date of this rule.

2.25. HIPAA Security Rules – means those security rules described in 45 C.F.R. Part 164, Subpart C, as modified and enlarged by the HITECH Act and any other subsequent amendments as of the date of this rule.

2.26. HITECH Act – means the Health Information Technology for Economic and Clinical Health Act of 2009, and its implementing rules promulgated at 45 C.F.R. Parts 160, 162, and 164.

2.27. Inquiry – means a request directed by a participating organization to the Network for the disclosure of a patient's protected health information for a permissible purpose. Inquiry involves the potential exchange of protected health information between multiple participating organizations.

2.28. Licensed Practitioner – means an individual licensed to provide health care items or services by a West Virginia board identified in Chapter 30 of the West Virginia Code, or by an equivalent board of another state.

2.29. Master Patient Index – means the index wherein personal demographic information of patients is securely maintained by the Network to record their decision to opt-out of the health information exchange. For those patients who have not elected to opt-out, the master patient index shall be used to match the patients with any inquiries seeking the exchange of protected health information for a permissible purpose. The Network shall maintain personal demographic information regarding all potential patients in this master patient index, even if the decision is made to opt-out, in order to minimize the possibility of improperly matching patients.

2.30. Mental Health Information – means any information obtained in the course of treatment or evaluation of any patient suffering from a mental or behavioral disorder, including but not limited to, diagnosis and treatment information, and any information that would specifically identify a patient as receiving mental health services. The term "Mental Health Information" has the same meaning as the term "confidential information" is defined in W.VA. Code §27-3-1 *et seq.*

2.31. Minimum Necessary – means that when requesting, using, or disclosing protected health information for a permissible purpose other than treatment or emergency treatment, a covered entity or a business associate shall limit protected health information to the minimum amount needed to accomplish the intended purpose of the request, use, or disclosure. The term "Minimum Necessary' has the same meaning as such term is defined in 45 C.F.R. Part 164, Subpart E.

2.32. Out-Of-Pocket Goods and Services – means any goods and services for which the participating organization has been paid out-of-pocket in full by the patient, and the patient has requested the participating organization to restrict the disclosure of those goods and services to an insurance company, group health plan, or other third party payor for payment or health care operations. The term "Out-of-Pocket-Goods and Services" has the same meaning as such term is defined in the HITECH Act.

2.33. Opt-Out – means a process under which any patient who does not consent to the use and disclosure of his or her protected health information with other participating organizations pursuant to the Network's health information exchange may affirmatively express his or her decision not to participate.

2.34. Participant or Participating Organization – means any health care provider, licensed practitioner, public health agency, health care clearinghouse, health plan, or other organization approved by the Network that establishes a contractual relationship with the Network in accordance with a standard participation agreement. A participant or participating organization must be a covered entity under HIPAA, a public health agency, or a business associate of a covered entity. Multiple covered entities operating as a single organized health care arrangement under 45 C.F.R. Part 160, may constitute a single participating organization upon approval of the Network. A participant or participating organization may be a full service participant, a data user, or a WV e-Directive Registry subscriber.

2.35. Patient – means the individual whose personal demographic information or protected health information is subject to electronic storage and transfer by the health information exchange. The term "Patient" includes a personal representative who has the authority to consent or authorize the disclosure of a patient's protected health information pursuant to 45 C.F.R. § 164.502(g) and any other applicable

state or federal laws. A patient may also register as an authorized user for access to the Network's patient portal through a cooperating participating organization.

2.36. Patient Notice – means a written notice prepared and approved by the Network, and supplied to its participating organizations for distribution to patients. The patient notice shall be provided to all patients during their first visit or encounter with a participating organization after it enrolls in the Network, and where possible, before the date of anticipated enrollment. The participating organization may provide the patient with an electronic version of the patient notice if the patient has specifically agreed to electronic notice as permitted by the HIPAA privacy rules. The patient may obtain a paper copy of the patient notice from the participating organization upon request. This patient notice shall explain the function of the Network; the permissible purposes for which a patient's protected health information may be shared with other participating organizations through the Network; the types of protected health information which may be shared with other participating organization; the need for the patient's consent to share certain categories of sensitive health information; the potential benefits and risks of participation in the Network; and the fact that a patient's participation in the Network is voluntary and subject to a patient's right to opt-out.

2.37. Patient Portal – means an on-line service offered by the Network through a cooperating participating organization which enables a patient to directly access and view only his or her protected health information from anywhere with a secure internet connection through the Network's health information exchange.

2.38. Patient Restricted Information – means any protected health information that is subject to a use or disclosure restriction impacting a permissible purpose, and that has been specifically requested by a patient and agreed to by a participating organization or data supplier pursuant to 45 C.F.R Part 164. It could also include a patient's request for restriction to a use or disclosure of protected health information permissible under state law.

2.39. Payment – means any activity undertaken to obtain or provide reimbursement for the provision of health care items or services to a patient. Payment also includes activities arising out of billing and collection, obtaining premiums for health plan coverage, determining eligibility for coverage, coordinating benefits with other health plans, performing health plan risk adjustment, reviewing medical necessity, providing precertification or preauthorization of services, and other similar transactions. The term "Payment" has the same meaning as such term is defined in 45 C.F.R. Part 164.

2.40. Personal Demographic Information – means information which may be used to individually identify a patient, but which excludes any and all clinical or health-related information. Personal demographic information may include, but not be limited to, the patient's name, address, Social Security number, date of birth, telephone number, and driver's license number.

2.41. Personal Health Record – means a health record that is established by a patient on his or her own behalf, and that uses an online platform sponsored by another entity. This personal health record may be developed by gathering and consolidating protected health information from many sources, including participating organizations of the Network's health information exchange.

2.42. Protected Health Information – means any information that relates to the past, present, or future physical or mental health or condition of a patient, the provision of health care items or services to the patient, and the past, present, or future payment for the provision of health care items or services to a patient. Protected health information also must personally identify a patient or provide a reasonable basis to believe that the information can be used to identify a patient. The term "Protected Health Information"

shall also include electronic protected health information and each shall have the meaning as defined in 45 C.F.R. Part 160.

2.43. Public Health Reporting – means the exchange of protected health information through the Network to a federal or state agency for the reporting and surveillance of specified health conditions as required or authorized by law, and for the reporting of immunization data. The reporting shall contain the minimum amount of protected health information or personal demographic information required or authorized for the reporting purpose.

2.44. Psychotherapy Notes – means notes recorded by a mental health care provider documenting or analyzing the contents of a conversation by a patient during a private, group, or family counseling session, and that are separated from the rest of the patient's medical record. The term "Psychotherapy Notes" has the same meaning as such term is defined in 45 C.F.R. Part 164.

2.45. Sensitive Health Information – means the subset of protected health information involving drug or alcohol abuse information, mental health information, psychotherapy notes, out-of-pocket goods and services, patient restricted information, or any other goods and services subject to heightened privacy and confidentiality requirements under federal and state laws or rules, or regulations and specifically approved by the Network.

2.46. Site Administrator – means an authorized user of the Network who is a member of the workforce of a participating organization, who may grant and terminate authorized user status, and who may perform other administrative functions within or on behalf of his or her participating organization. A participating organization may designate more than one site administrator.

2.47. Treatment – meant the provision of health care items or services to a patient, including direct patient care as well as consultation, coordination, management, or patient referral between or from one participating organization to another. The term "Treatment" has the same meaning as the term is defined in 45 C.F.R. Part 164. Unless stated otherwise, treatment shall be limited to the provision of health care items or services to the patient who is the subject of the information (except in the case of mother/infant).

2.48. Unsecured protected health information – means protected health information that has not been rendered unusable, unreadable, or indecipherable by unauthorized individuals or entities through the use of encryption or other federally-approved technology. The term "Unsecured Protected Health Information" has the same meaning as such term is defined in 45 C.F.R. Part 164.

2.49. WV e-Directive Registry – means a service by which participating organizations that are health care providers may access a patient's advance directive forms, physicians' orders for scope of treatment (POST) forms, and do not resuscitate cards. A participating organization that seeks access to these documents must be a WV e-Directive Registry subscriber.

2.50. WVDirect – means a service that offers a secure messaging platform to transmit protected health information and other data to other WVDirect subscribers via electronic mail. WVDirect's secure messaging platform is offered as a separate and distinct service from the Network's health information exchange. A health care provider does not have to become a participating organization to subscribe to WVDirect, but must be a WVDirect subscriber.

2.51. West Virginia Health Information Network or Network – means the public-private partnership created by West Virginia Code Chapter 29G, and which has as one of its purposes to develop

an interoperable health information exchange in West Virginia. The Network also offers services that are separate and distinct from the health information exchange, including WVDirect.

2.52. Workforce – means employees, contractors, volunteers, trainees, or other persons whose conduct, in the performance of work for a participating organization, is under the direct control of the participating organization, whether or not they are paid by the participating organization. The term "Workforce" has the same meaning as the term is defined in 45 C.F.R. Part 160.

§65-28-3. The Health Information Exchange.

3.1. The Network shall establish an interoperable statewide network for the disclosure and use of protected health information by and between participating organizations to improve the efficiency, quality, and integration of health care delivery, and to improve health care outcomes, all of which shall be considered to be in the best interests of patients pursuant to West Virginia Code §16-29G-8. Protected Health Information may be disclosed and used through the health information exchange unless and until the patient has expressed an affirmative choice to opt-out.

3.2. The Network shall maintain the privacy and security of the health information exchange in accordance with all applicable federal and state laws or rules, or regulations, including but not limited to, HIPAA, the HIPAA privacy rules, the HIPAA security rules, and the HITECH Act. This privacy and security shall apply not only to protected health information being exchanged through the Network, but shall also apply to any protected health information maintained by the Network in its master patient index or otherwise.

3.3. There may be two types of protected health information transactions recognized by the Network's health information exchange.

3.3.a. One type may involve the submission of an inquiry by one participating organization seeking the disclosure of available protected health information on a particular patient from all other participating organizations, such as an inquiry for treatment purposes; and

3.3.b. The other type may involve the point-to-point disclosure of protected health information between two (2) participating organizations, such as in payment, clinical messaging, or public health reporting.

3.4. Both an inquiry and a point-to-point transaction submitted by a participating organization shall designate a permissible purpose for which protected health information may be disclosed and used.

3.5. The Network shall not sell protected health information to third parties for marketing or other commercial purposes without the prior written authorization of the affected patient.

3.6. The secure messaging service offered by the Network known as WVDirect is a separate and distinct service from the Network's health information exchange.

§65-28-4. Permissible Purposes for Health Information Exchange.

4.1. The placement of appropriate limits upon health information exchange shall minimize the potential for misuse or abuse of protected health information, thereby enhancing patient and participating organization confidence in the health information exchange process. Accordingly, the permissible purposes for which protected health information may be disclosed and used through the Network shall be limited by the Network. Permissible purposes may include treatment, emergency treatment, payment,

health care operations, public health reporting, or any other purpose specifically authorized by federal and state laws or rules, or regulations, or approved by the Network.

4.2. Absent a permissible purpose, no person or participating organization shall seek the disclosure of protected health information through the Network's health information exchange.

4.3. A participating organization may submit an inquiry to the Network for the protected health information of a patient for a permissible purpose if it has a relationship to the patient sufficient to justify the permissible purpose. For example, a participating organization may submit an inquiry for treatment purposes when the participating organization is actually involved in the treatment of the patient. The Network shall implement a master patient index and a record locator function to identify which participating organizations possess protected health information responsive to an inquiry.

4.4. A participating organization may submit a point-to-point transaction for a permissible purpose if it has a relationship to the patient sufficient to justify the permissible purpose. For example, a participating organization treating a patient may order and receive the patient's laboratory tests results in the form of a clinical message from another participating organization or data supplier.

§65-28-5. Patient Opt-Out.

5.1. The Network shall provide a patient with a reasonable and meaningful opportunity as set forth in this rule to make an informed choice about whether his or her protected health information may be disclosed and used in the Network's health information exchange.

5.2. Any patient who does not want to consent to the disclosure and use of his or her protected health information in the health information exchange may elect to opt-out. Affirmative action by the patient is not necessary when a patient consents to his or her participation in the Network's health information exchange.

5.3. To ensure that patients are able to make an informed choice, participating organizations shall provide each patient with educational information during the first patient encounter after the participating organization enrolls in the Network's health information exchange. Where possible, patients may be provided with the educational information prior to the enrollment of the participating organization in the Network's health information exchange. This educational information shall be provided in writing, and if necessary, in any other format (on-line presentation, verbal counseling, foreign language presentation, etc.) designed to ensure that its contents are communicated to and understood by the patient.

5.4. This educational information shall consist of, at a minimum, a written patient notice developed by the Network which explains in plain language:

5.4.a. The function of the Network's health information exchange;

5.4.b. The permissible purposes for which a patient's protected health information may be disclosed to and used by other participating organizations through the health information exchange;

5.4.c. The types of protected health information which may be disclosed to other participating organizations;

5.4.d. The need for the patient's specific written authorization to disclose certain categories of sensitive health information;

5.4.e. The fact that a patient's personal demographic data shall be included in a master patient index maintained by the Network to permanently record his or her consent decision;

5.4.f. The potential benefits and risks of participation in the Network; and

5.4.g. The fact that a patient's participation in the Network is voluntary and subject to a patient's right to opt-out.

5.5. The written patient notice may be provided to the patient as an addendum to a participating organization's notice of privacy practices. The participating organization is encouraged to record the delivery of the patient notice in the patient's medical record.

5.6. In addition to the written patient notice, the Network shall also undertake the following efforts to educate and publicly notify patients of the existence and operation of its health information exchange:

5.6.a. The Network shall publish its written patient notice and a list of all then current participating organizations during the first week of January, April, July, and October of each year in the State Register.

5.6.b. The Network shall publish its written patient notice in the form of a Class III legal advertisement in at least one qualified newspaper of general circulation, as defined by W.Va. Code §59-3-1 *et seq.* in each defined area that the Network intends to serve, as well as the expected date of implementation in each defined area. This Class III legal advertisement shall be published at least thirty (30) days prior to the date upon which the Network's health information exchange becomes operational in the defined area;

5.6.c. The Network shall prepare and distribute educational posters for display by its participating organizations in public areas that are designed to inform patients about the health information exchange and their right to opt-out of the exchange;

5.6.d. The Network shall include the written patient notice, as well as other educational information designed to inform patients about the health information exchange and their right to opt-out, on its internet website. At this website, the Network may include the capability for a patient to opt-out of the health information exchange. The Network shall also require participating organizations to include the written patient notice on their internet websites, if any; and

5.6.e. The Network shall encourage prospective participating organizations to begin the distribution of the written patient notice at each of its patient encounters, to include the written patient notice on its own internet website, and to display the Network's educational posters in public areas of its facility.

5.7. A patient shall be considered an active participant in the health information exchange until and unless he or she opts-out. A patient becomes an active participant for all purposes after the enrollment of his or her participating organization in the Network's health information exchange, or after a data supplier discloses or otherwise makes available his or her protected health information for access through the Network's health information exchange.

5.8. A patient may opt-out of the health information exchange during a patient encounter with a participating organization, or if available on the Network website, by registering his or her decision to

opt-out on-line. Both data users and full service participants must offer patients the opportunity to opt-out.

5.9. A participating organization shall communicate a patient's decision to opt-out immediately, and the Network shall permanently record that decision in a master patient index maintained by the Network. The Network shall maintain personal demographic information regarding all potential patients in this master patient index, even if the decision is made to opt-out, in order to minimize the possibility of improperly matching patients.

5.10. A patient may elect to opt-out of the health information exchange at any time, even after having been already a participant. However, any exchange of protected health information that may have occurred prior to a patient's decision to opt-out shall not be reversed.

5.11. For a patient who has opted-out, the Network shall not disclose protected health information through the health information exchange except for public health reporting to a state or federal agency.

5.12. A patient may revoke his or her decision to opt-out of the health information exchange at any time by completing a revocation form developed and approved by the Network. A patient's election to revoke his or her decision to opt-out may be accomplished either during a patient encounter at a participating organization, or if available, on-line at a website maintained by the Network.

§65-28-6. Patient Rights.

6.1. The Network shall develop, implement, and operate its health information exchange in a manner that is both transparent and patient-centered;

6.1.a. All of the Network's forms and educational materials shall be written in plain language;

6.1.b. All of the Network's forms and educational materials shall be made readily accessible to patients free of charge either electronically, or at the request of the consumer, in paper format; and

6.1.c. All meetings of the Network's board of directors shall be conducted in compliance with the West Virginia Open Governmental Proceedings Act in W.Va. Code §6-9A-1 *et seq.*

6.2. A participating organization shall not deny care to any patient solely because he or she elects to opt-out of the health information exchange.

6.3. A patient may register for access to the Network's patient portal with a cooperating participating organization. A patient portal may be used by the patient to directly access the health information exchange and view his or her protected health information from a participating organization or data supplier.

6.4. Absent a patient portal, a patient may access his or her protected health information consistent with the requirements of the HIPAA privacy rules, the HITECH Act, and W.Va. Code §16-29-1 *et seq.* Participating organizations are the originators of the protected health information, and maintain the designated record sets in which the protected health information resides. Accordingly, the participating organization whose designated record set is subject to a request for access by a patient is

responsible for evaluating and responding to the request. The Network shall direct the patient to present the request for access to the applicable participating organization for processing.

6.4.a. The participating organization is solely responsible for making all determinations regarding the grant or denial of the patient's request for access.

6.4.b. If access is granted, the participating organization is responsible for providing access from its own designated record set.

6.5. A patient may amend his or her protected health information consistent with the requirements of the HIPAA privacy rules and the HITECH Act. Participating organizations are the originators of the protected health information, and maintain the designated record sets in which the protected health information resides. Accordingly, the participating organization whose protected health information is subject to a request for amendment by a patient is responsible for evaluating, responding to, approving, or disapproving any request. The Network shall direct the patient to present the request for amendment to the applicable participating organization for processing. An amendment cannot be accomplished via the patient portal.

6.5.a. The participating organization is solely responsible for making all determinations regarding the grant or denial of the patient's requested amendment, and for ultimately providing for the amendment within its own designated record set; and

6.5.b. Any participating organization that agrees to an amendment shall make it available to the Network for the purposes of the health information exchange.

6.6. A patient has a right to an accounting of disclosures of his or her protected health information consistent with the requirements of the HIPAA privacy rules and the HITECH Act. The Network shall track electronically all disclosures made through its health information exchange.

6.6.a. If a request for an accounting of disclosures is received by the Network from a patient or participating organization, the Network shall prepare the accounting from it health information exchange consistent with the requirements of the HIPAA privacy rules and the HITECH Act, and deliver the accounting to the applicable participating organization.

6.6.b. The participating organization is responsible for delivering the Network's accounting of disclosures, along with the participating organization's own accounting of disclosures, to the patient. An accounting of disclosures cannot be accomplished via the patient portal.

6.7. A patient may request a restriction on the disclosure of any protected health information for the permissible purposes of payment and health care operations relating to goods or services for which a patient has paid a participating organization out-of-pocket, in full, in accordance with the requirements of the HITECH Act. In addition, a patient may request other restrictions upon the use and disclosure of his or her protected health information subject to the agreement of the patient's participating organization in accordance with the HIPAA privacy rules. The Network shall comply with any and all restrictions by accepting a participating organization's classification of the protected health information as sensitive health information pursuant to Section 7 of this rule.

6.7.a. The participating organization is responsible for identifying, classifying, segregating, and blocking any protected health information relating to out-of-pocket goods and services as sensitive health information; and

6.7.b. Patient restricted information shall likewise be identified, classified, segregated, and blocked by the participating organization as sensitive health information.

6.8. A patient has the right to be notified of a breach of his or her unsecured protected health information consistent with the requirements of the HITECH Act and W.Va. Code §46A-2A-1 *et seq.* The Network shall comply fully with its notification obligations under these federal and state laws.

6.9. The Network shall affiliate with at least one vendor of a personal health record product. If a patient establishes a personal health record, that personal health record may contain protected health information obtained from his or her patient portal. Absent access to a patient portal, a patient may instead seek access to his or her protected health information from each participating organization in accordance with Section 6.4 for inclusion in his or her personal health record.

§65-28-7. Sensitive Health Information

7.1. Federal and state laws impose heightened privacy and confidentiality requirements upon the disclosure and use of certain types of protected health information that may be considered particularly private or sensitive to a patient. The categories of sensitive health information may include:

7.1.a. Drug or alcohol abuse information;

7.1.b. Mental health information;

7.1.c. Psychotherapy notes;

7.1.d. Out-of-pocket goods and services;

7.1.e. Patient restricted information; and

7.1.f. Any other goods and services subject to heightened privacy and confidentiality requirements under federal and state laws, rules, or regulations and specifically approved by the Network.

7.2. The Network shall provide a method by which participating organizations and data suppliers may identify, classify, segregate, and block the routine disclosure of sensitive health information through the health information exchange. Each participating organization and data supplier is solely responsible for identifying, classifying, segregating, and blocking the disclosure of sensitive health information contained in its designated record sets through the health information exchange.

7.3. The Network may develop written standards, forms, or protocols by which a patient may specifically authorize the disclosure of his or her sensitive health information consistent with all legal requirements. These standards, forms, and protocols may be established either as part of or separate from the health information exchange.

§65-28-8. Participating Organizations.

8.1. In order to request and receive a patient's protected health information through the Network's health information exchange; it is necessary to first become a participating organization. The Network may in its discretion grant participating organization status to any health care provider, licensed practitioner, public health agency, health care clearinghouse, health plan or other organization that establishes a contractual relationship in accordance with a standard participation agreement developed

and approved by the Network. A participating organization may take the form of either a data user or a full service participant.

8.2. During the course of its development and implementation, the Network shall establish a plan for statewide coverage that is consistent with its available resources and the readiness of prospective participating organizations to connect to the health information exchange.

8.2.a. To evaluate the readiness of prospective participating organizations to connect to the Network, the Network shall prepare and publish interoperability guidelines that shall be met in order to become a participating organization.

8.2.b. The Network's interoperability guidelines shall be based upon national and industry health data and security standards regarding interoperability between and among participating organizations.

8.2.c. The Network's interoperability guidelines shall be designed reasonably to ensure that protected health information made available through the health information exchange is complete, accurate, and current.

8.3. A full service participating organization shall enable the Network to access personal demographic information and protected health information about all of its patients, and to include these patients in the Network's master patient index, subject to each patient's right to opt-out of the health information exchange. Any data supplier approved by the Network shall likewise promptly enable the Network to access personal demographic information and protected health information.

8.4. A participating organization and a data supplier shall thereafter promptly transmit to the Network any known changes to its patients' personal demographic information to maintain the accuracy of the master patient index.

8.5. The Network may in its discretion grant participating organization status to health care providers or licensed practitioners that cannot comply with the Network's interoperability guidelines in order to provide the health care providers or licensed practitioners with access to the protected health information of their patients maintained by other participating organizations for a permissible purpose. These organizations shall be known as data users. Because the purpose of the Network is to improve the efficiency, quality, and integration of health care delivery, and to improve health care outcomes, such purpose is necessarily dependent upon interoperability and the sharing of data between the maximum number of participating organizations. Accordingly, the Network may impose upon any data user reasonable time limitations or conditions, or both, which require the data user to ultimately come into compliance with the Network's interoperability guidelines and become a full service participant.

8.6. A participating organization shall strictly control access to the Network's health information exchange by its workforce through an organized system of approving and designating authorized users.

8.7. Each participating organization and data supplier is solely responsible for identifying, classifying, segregating, and blocking the disclosure of sensitive health information contained in its designated record sets through the Network's health information exchange.

8.8. A participating organization may disclose and use protected health information as part of the health information exchange only in a manner that is consistent with the following:

8.8.a. HIPAA, the HIPAA privacy rules, the HIPAA security rules, the HITECH Act, and any other applicable federal law or regulation;

8.8.b. Any applicable West Virginia law or legislative rule, including but not limited to, this legislative rule; and

8.8.c. the Network-approved participation agreement.

8.9. Each participating organization shall designate a site administrator from its workforce to be the primary point of contact with the Network, and to perform various administrative functions, including but not limited to, granting and terminating authorized user status to members of its workforce.

8.10. A participating organization shall promptly report any malfunctions, misuse, or breach involving the health information exchange to the Network, or its designee, for investigation and remediation.

§65-28-9. Authorized Users.

9.1. The Network and each participating organization shall designate authorized users based upon job roles fulfilled by individuals in their respective workforces. Each participating organization is responsible for establishing this role-based access system to limit access within an organization to those workforce members with a need to know.

9.2. Each participating organization shall designate, maintain, and certify their official lists of authorized users to the Network. A workforce member may be designated as an authorized user only if that member requires access to protected health information in the Network's health information exchange in order to perform his or her job responsibilities within the participating organization.

9.3. A workforce member who is not designated as an authorized user may not access the Network for any purpose.

9.4. Each participating organization shall provide training for its authorized users before they may access the health information exchange. This training program shall include a review of the functionality of the health information exchange, as well as a review of all rules, policies, and procedures promulgated by the Network.

9.5. Each participating organization is responsible for maintaining an appropriate and current list of its authorized users. This requires that changes in employment status as well as other workforce changes, including termination of authorized user status, shall be communicated immediately and electronically to the Network by the participating organization's site administrator.

9.6. The Network shall require any of its subcontractors and vendors that qualify as a business associate under HIPAA and the HITECH Act to also designate, maintain, and certify their list of authorized users in accordance with the role-based access concept.

9.7. A patient may seek approval for authorized user status if he or she registers for access to the Network's patient portal with a cooperating participating organization to directly access and view only his or her protected health information that has been contributed to the health information exchange by any participating organization or data supplier.

9.8. The Network may temporarily suspend or permanently revoke an individual's status as an authorized user of the Network for any of the following reasons;

9.8.a. Violation of this rule;

9.8.b. Violation of any federal or state law or rule, or regulation;

9.8.c. Fraudulent activity;

9.8.d. Prolonged inactivity on the health information exchange system; or

9.8.e. Any other good cause.

§65-28-10. User Authentication.

10.1. To optimize the privacy and security of its health information exchange, the Network shall ensure that an authorized user's identity is properly authenticated each time the exchange is accessed. The Network shall establish a system by which each participating organization shall implement minimum requirements for authentication information unique to each authorized user in accordance with industry standards and specifications.

10.2. The Network and the participating organizations shall place strict controls upon the use of authentication information. An authorized user to whom authentication information is assigned shall not share his or her authentication information with any other individual.

10.3. An authorized user shall immediately report any loss or misuse of his or her authentication information to the participating organization or to the Network, as applicable.

10.3.a. The Network and the participating organization's site may lock out the affected authorized user from accessing the health information exchange; and

10.3.b. This lock out shall be terminated only after an authorized user's identity is verified, and new authentication information has been approved for the authorized user in question.

§65-28-11. Minimum Necessary.

11.1 The HIPAA privacy rules apply a "minimum necessary' standard to many types of disclosures and uses of protected health information. This standard essentially means that a covered entity or business associate must make reasonable efforts to limit the disclosure and use of protected health information to the minimum necessary to accomplish the purpose of the proposed disclosure and use.

11.1.a. The minimum necessary standard is subject to certain exceptions:

11.1.a.1. The minimum necessary standard shall not apply to any disclosures and uses of protected health information for the permissible purposes of treatment or emergency treatment;

11.1.a.2. The minimum necessary standard shall not apply to disclosures and uses of protected health information pursuant to a signed authorization by the patient; and

11.1.a.3. The minimum necessary standard shall not apply to disclosures of protected health information pursuant to a patient's request for access to his or her own protected health information, such as through a Network patient portal on the Network's health information exchange.

11.2. The Network shall not apply the minimum necessary standard to any of the exceptions in subdivision 11.1.a. of this section under its health information exchange.

11.3. Participating organizations shall limit their inquiry for protected health information under the Network to the minimum necessary when required under the HIPAA privacy rules.

11.4. The Network shall rely upon the reasoned judgment and representations of a participating organization seeking access to protected health information as complaint with the minimum necessary standard under HIPAA privacy rules.

11.5. The Network may develop standard protocols or data fields which are designed to disclose only the minimum necessary amount of protected health information to accomplish a permissible purpose. For example, only those data fields required or authorized by federal or West Virginia law to comply with a public health reporting requirement may be employed by the Network to accomplish this reporting. The Network may investigate other permissible purposes for which standard protocols or data fields designed to disclose only the minimum necessary amount of protected health information may be developed.

§65-28-12. Business Associates; De-Identification of protected health information.

12.1. Under the HITECH Act, the Network's operation of a health information exchange qualifies it as a business associate of its various participating organizations, data suppliers, and WVDirect subscribers. Accordingly, the Network shall enter into a valid and binding business associate agreement with each participating organization, data supplier, and WVDirect subscriber. The business associate agreement shall comply with any and all of the requirements of HIPAA and the HITECH Act.

12.2. If the Network uses subcontractors and vendors to assist it with the development, implementation, and operation of the health information network, and the subcontractors and vendors fall within the definition of a business associate under HIPAA and the HITECH Act, then the Network shall enter into a valid and binding business associate agreement with each subcontractor or vendor. The business associate agreement shall comply with all of the requirements of HIPAA and the HITECH Act.

12.3. The HIPAA privacy rules identify the means by which protected health information may be deidentified. To be considered as deidentified, the remaining data shall not identify a patient, and there shall be no reasonable basis to believe that the information can be used to identify a patient. The Network may deidentify protected health information, and may disclose or use the deidentified data for any public health or research purpose approved by the Network board.

§65-28-13. Security Safeguards.

13.1. The Network shall develop and implement appropriate administrative, physical, and technical safeguards designed to protect the privacy and security of any protected health information and personal demographic information that it receives, creates, discloses, or uses under its health information exchange.

13.2. At a minimum, these security safeguards shall comply with the requirements set forth in the HIPAA security rules codified at 45 C.F.R. §§164.306, 164.308, 164.310, 164.312, and 164.316.

13.3. The Network's development and implementation of security safeguards shall remain consistent over time with new developments and changes. Accordingly, the intent of the Network is that the safeguards required by the HIPAA security rules are minimum safeguards. When necessary or appropriate, these safeguards may be amended, modified, or enhanced to keep pace with evolving technologies, new industry standards, and legal requirements that may become applicable in the future.

§65-28-14. Complaint Procedure.

14.1 Any patient, authorized user, or participating organization, may file a written complaint with the Network concerning any aspect of its operations. All complaints shall be in writing and shall identify the individual responsible for making the complaint.

14.1.a. The Network shall develop and approve a complaint form which includes, at a minimum, the following items:

14.1.a.1. The name, address, and phone number of the individual making the complaint;

14.1.a.2. The date of the complaint;

14.1.a.3. The date that an adverse event occurred; and

14.1.a.4. A description of the adverse event.

14.2. The Network shall designate a person responsible for receiving, investigating, and responding to complaints. This complaint procedure shall be prominently featured on the website maintained by the Network, along with the name and address of the person designated by the Network to handle complaints.

14.3. The Network shall acknowledge receipt of a complaint, investigate it, and make every effort to resolve the complaint within a reasonable time frame, which in most cases shall not exceed thirty (30) days.

14.4. The Network shall notify the complaining individual of the Network's resolution or other response to the complaint in writing. This resolution or response shall include information about how the individual may forward the complaint to the Executive Director of the West Virginia Health Care Authority if it has not been resolved to the satisfaction of the complaining individual.

14.5. The Network shall periodically analyze all filed complaints to determine if persistent or recurrent problems exist with the health information exchange system or its operation.

§65-28-15. Pilot Demonstration Projects.

15.1. The Network may develop, implement, and operate one or more pilot demonstration projects in designated communities of the state to acclimatize participating organizations to the health information exchange environment, and to evaluate the efficiency and effectiveness of its health information exchange system. The Network shall coordinate its pilot demonstration projects with diverse

components of the health care delivery system in the communities chosen. The pilot demonstration projects shall be developed, implemented, and operated in full compliance with this rule.