

WVHIN's Privacy and Security Framework

Consumer/Employer/Privacy Committee
John Wiesendanger, Committee Chair

I. POLICY OPTIONS – INDIVIDUAL RIGHTS/PARTICIPATION

A. The WVHIN must develop and implement comprehensive policies and procedures designed to assist network participants in safeguarding the following consumer rights:

- ◆ The right of access to their PHI
- ◆ The right to seek an amendment of their PHI
- ◆ The right to an accounting of disclosures of their PHI
- ◆ The right to agreed-upon disclosure restrictions and alternative communication methods involving their PHI

B. The WVHIN must develop and implement comprehensive policies and procedures designed to provide consumers with the right to file a complaint and to receive a response to such a complaint

II. POLICY OPTIONS – CONSUMER NOTICE

A. The WVHIN must develop a standard addendum to be included within the Notice of Privacy Practices of all network participants that informs consumers of the following:

- ◆ Their chosen network participant is a member of an electronic health information exchange sponsored by the WVHIN
- ◆ Their PHI will be stored, used, and disclosed in an electronic format
- ◆ The utilization of an electronic format will not change any of their legal rights under existing law regarding the confidentiality, privacy, or security of their PHI
- ◆ Their PHI will not be disclosed by their chosen network participant to other network participants seeking access to their PHI via the health information exchange without their consent, either by exercise of an opt-out option or by some other meaningful consumer choice option (see Policy Option V.A)

B. The WVHIN must develop and implement comprehensive policies and procedures designed to make its operation both transparent and consumer-friendly, including the following:

- ◆ All policies and procedures will be written in plain language
- ◆ All policies and procedures will be made readily accessible to consumers free of charge either electronically, or at the request of the consumer, in paper format
- ◆ All meetings of the WVHIN board of directors shall be conducted in compliance with the West Virginia Open Governmental Proceedings Act

C. The WVHIN must devote substantial resources to the development and implementation of an educational outreach initiative designed to inform consumers about their rights, the operation of the WVHIN, how and when their PHI may be used and disclosed by the WVHIN, and what is being done to safeguard the confidentiality, privacy, and security of their PHI by the WVHIN

D. The WVHIN must develop and implement comprehensive policies and procedures identifying the various circumstances under which a breach of privacy or confidentiality of PHI must be reported to affected network participants, and directly to individual consumers, in order to promote the transparency and accountability of the WVHIN.

III. POLICY OPTIONS – MINIMUM NECESSARY/LIMITED USE

A. The WVHIN must develop standard data fields that are designed to support “minimum necessary” principles for transactions by network participants, especially for common standard transactions like:

- ◆ Payment
- ◆ HIPAA-defined health care operations (e.g. quality assessment, peer review, underwriting, compliance programs, legal and accounting services, business planning and management activities, etc.)
- ◆ Coordination of benefits
- ◆ Plan eligibility
- ◆ Pre-authorization and certification

B. The WVHIN must develop and implement comprehensive policies and procedures designed to support compliance with HIPAA “minimum necessary” requirements by network participants, except in the following situations:

- ◆ Disclosures of PHI to provider for treatment purposes
- ◆ Disclosures to consumers of their own PHI
- ◆ Disclosures made pursuant to HIPAA-compliant authorizations
- ◆ Disclosures required by law

IV. **POLICY OPTIONS – SECURITY SAFEGUARDS**

A. The WVHIN must develop and implement comprehensive policies and procedures designed to provide reasonable and appropriate “centralized” security safeguards for the PHI of consumers, including but not limited to, the following:

- ◆ Comprehensive staff training
- ◆ Encryption of PHI at rest within the network, if appropriate, and when transmitted from one network participant to another
- ◆ Audit logs for any PHI that is accessed or attempted to be accessed
- ◆ Standard protocols for identifying and authenticating individual consumers
- ◆ Standard protocols for identifying and authenticating those given access to PHI

B. The WVHIN must develop and implement comprehensive policies and procedures designed to require “federated” security safeguards to be implemented by network participants as well, thereby creating security redundancy within the health information exchange network.

C. The WVHIN must establish a process for facilitating security collaboration between the WVHIN and network participants in the following areas:

- ◆ Identification of significant threats
- ◆ Review and discussion of alleged and real security incidents
- ◆ Incident response, reporting, and remediation

V. POLICY OPTIONS – CONSUMER CONSENT AND AUTHORIZATION

A. The WVHIN must develop and implement comprehensive policies and procedures designed to allow consumers to consent to the disclosure of their PHI by their chosen network participant to other network participant seeking access to their PHI via the health information exchange network, and such consent may be accomplished by either an opt-out option or by some other meaningful consumer choice option.

B. The WVHIN must develop and implement comprehensive policies and procedures designed to allow it to use and disclose PHI in the following circumstances without the need for a written or electronic authorization signed by the consumer:

- ◆ Uses and disclosures by or to a network provider for treatment purposes
- ◆ Uses and disclosures by or to a network health plan for payment purposes
- ◆ Uses and disclosures by or to a network participant for its legitimate health care operations as defined by HIPAA

C. The WVHIN must develop and implement comprehensive policies and procedures designed to require written or electronic authorizations signed by consumers for all disclosures of their PHI that are not identified under federal or state law as being exempt from such a requirement, including but not limited to, the following:

- ◆ Mental health PHI
- ◆ Substance abuse and alcohol abuse treatment PHI
- ◆ HIV/AIDS testing and treatment PHI
- ◆ Sexually transmitted disease PHI (as to minors)

D. The WVHIN must develop and implement comprehensive policies and procedures designed to prevent its unauthorized use, disclosure, and/or sale of consumers' PHI for marketing or other commercial purposes.

VI. POLICY OPTIONS – GLOBAL CONSIDERATIONS

A. The WVHIN must develop and implement comprehensive policies and procedures designed to comply with all applicable laws and regulations.

B. The WVHIN must develop and implement comprehensive policies and procedures designed to comply with the requirements applicable to Business Associates under HIPAA.

C. The WVHIN must develop and implement comprehensive policies and procedures designed to ensure that any agents or subcontractors to whom it provides PHI agree to the same restrictions and conditions that apply to the WVHIN.

D. The WVHIN shall seek guidance from the requirements applicable to Business Associates under HIPAA, as well as from generally accepted industry standards, when addressing a particular privacy or security concern for which there exists no more restrictive law or regulation, or no more restrictive policy or procedure specifically approved by the WVHIN.
