Policies and Procedures

Effective: October 22, 2022
Revised: July 23, 2025

Table of Contents

West Virginia Health Information Network ("WVHIN") Policies and Procedures 1
Table of Contents 2
Background 4
1. Authorized Users 4
1.1 Background, Purpose, and General Requirements 4
1.2 Limitation of Access to Data 4
1.3 Identification, Verification, Management, and Changes to Authorized Users 5
1.4 Training 5
1.5 The WVHIN's Rights and Responsibilities 6
2. Authentication of Authorized Users 6
2.1 Background and Purpose 6
2.2 User Names and Passwords Generally 6
2.3 Password Convention 7
2.4 Lock Outs; Password Resets; Reporting Unauthorized Use 7
3. Authorized User and Participating Organization Data Access and Use 7
3.1 Participating Organization's Policy Obligations 7
3.2 Minimum Necessary; Exceptions to Minimum Necessary 7
3.3 Data Misuse 8
3.4 Discipline for Non-Compliance 8
4. Patient Access and Rights 8
4.1 Patient's Right of Access to Data 8
4.2 Patient's Right to Accounting of Disclosures 9
4.3 Patient Notice, Patient Consent, and Opt-Out Rights 9
4.4 Patient's Right to Amend Protected Health Information 11
4.5 Patient's Right to Request Restrictions on the Use or Disclosure of Own Protected Health Information 11
5. Permissible Purposes 12
5.1 Background; Permissible Purposes Generally 12
5.2 Permissible Purpose of Treatment 12
5.3 Permissible Purpose of Emergency Treatment 12
5.4 Permissible Purpose of Payment 12
5.5 Permissible Purpose of Limited Health Care Operations 13
5.6 Permissible Purpose of Public Health Reporting 14
5.7 Modification of Permissible Purposes; Public Health Use Cases 14
5.8 Uses and Disclosures by Non-Participant Third Parties 14
5.9 Deidentified Data 15
6. Business Associates and Business Associate Agreements 16
6.1 Business Associates; Business Associate Subcontractors 16
6.2 Business Associate Agreements 16
7. Data Contributor Responsibilities 17
7.1 Testing and Validation 17
7.2 Data Availability 17
8. Sensitive Health Information 17
8.1 Background and Purpose 17
8.2 Substance Use Disorder Information 18
8.3 Psychotherapy Notes 18
8.4 Out-Of-Pocket Goods and Services 19
8.5 Patient-Restricted Information 19
9. Interstate Data Exchange 19
9.1 National Networks 19
9.2 TEFCA 20
10. Data Controls 20
10.1 Privacy and Security 20

10.2 Data Consumption 20
10.3 Data Retention 20
10.4 Return of Data 21
11. Systems Operations and Services 21
11.1 Hardware and Software 21
11.2 Availability and Network Monitoring 21
11.3 Maintenance 21
12. Help Desk 21
13. Audit 22
14. Breach Notification 22
14.1 Background and Purpose 22
14.2 Obligations of Participating Organizations 23
14.3 Obligations of the WVHIN 23
15. Complaint Handling 24
16. Provider Authorization 25
17. Standards 25
18. Policies and Procedures Amendments 25

Background

The West Virginia Health Information Network, Inc. (the "WVHIN") was created by the West Virginia Legislature in 2006 under the oversight of the West Virginia Health Care Authority. Its purpose is to promote the design, implementation, operation, and maintenance of a fully interoperable statewide network to facilitate public and private use, and disclosure of health care information in the state. In 2017, the West Virginia Legislature transferred the operation of the WVHIN from state government to a new private, nonprofit corporation. The transfer was finalized effective January 1, 2018.

These policies and procedures (hereafter the "Policies and Procedures") contain requirements and specifications guiding the operation and use of the WVHIN Services (as further defined and detailed in Section 10 of these Policies and Procedures) and are consistent with and/or supplement the terms and conditions set forth within the WVHIN's standard participation agreement (the "Participation Agreement"). These Policies and Procedures may be amended from time to time. Participating Organizations are responsible for reviewing other relevant documents and policies on the WVHIN website and for otherwise monitoring the WVHIN website on a regular basis for updates. Any terms not otherwise herein defined shall have the meanings ascribed to them in the "Glossary," which is available on the WVHIN website.

1. Authorized Users

1.1 Background, Purpose, and General Requirements

Each Participating Organization shall maintain policies and procedures which control access by the Participant's Workforce to HIPAA-covered data within WVHIN. Authorized Users may include only those members of the Participating Organization's Workforce who require access to the Health Information Exchange to facilitate the use and disclosure of Protected Health Information for a Permissible Purpose (as further specified in Section 5 of these Policies and Procedures) as part of their job responsibilities. Authorized Users include Health Care Providers, Health Plans, Care Management Organizations, employees, staff, and other Workforce members of Participating Organizations who have been designated as needing access to the WVHIN Services to perform their job function. Access to the various WVHIN Services is dependent on the job function each Authorized User holds within his or her Participating Organization and the defined level of access assigned to each by the Participating Organization's own policies and procedures. Except when involved in the provision of Treatment, an Authorized User must only be given access to the minimum amount of Protected Health Information necessary to perform his or her role.

The following individuals may become an Authorized User:

- Workforce members of any Participating Organization;
- Workforce members of the WVHIN; and
- Workforce members of the WVHIN's Business Associates.

1.2 Limitation of Access to Data

While generalized policies and procedures controlling access to the WVHIN's Health Information Exchange by Workforce members are the responsibility of the Participating Organizations, the WVHIN reserves the right to require specific credentials in order to access certain data in the Exchange. Specific limitations on accessing certain types of Protected Health Information exists for the following:

- Only Licensed Practitioners with a Drug Enforcement Agency ("DEA") and National Provider Identifier ("NPI") may access data from prescription drug or Substance Use

Monitoring Program;
- ► Health Plans may only access data on Patients who are on their submitted panels;
- ► Health Plans may not access data for Treatment or Emergency Treatment purposes;
- ► Health Plans may only access data from the WV e-Directive Registry for Limited Health Care Operations;
- ► Care Management Organizations may not access data for Emergency Treatment purposes;
  and
- ► No Participating Organization may access data on a Patient who has Opted-Out of the WVHIN, except for a Public Health Reporting purpose.

1.3 Identification, Verification, Management, and Changes to Authorized Users

It is the responsibility of each Participating Organization to identify and verify its Authorized Users. Identifying information for each Authorized User must be provided to the WVHIN upon request. A Participating Organization may include as Authorized Users those individuals on its Workforce who require access to the WVHIN to perform their roles within the Participating Organization for a Permissible Purpose recognized by the WVHIN or as otherwise required by applicable law. Its Workforce will include employees, volunteers, and other persons whose work performance is under the direct control of the Participating Organization, regardless of whether they are paid by the Participating Organization. In addition, a Licensed Practitioner who is a credentialed medical staff member of a Participating Organization, and who maintains Treatment relationships with Patients at its facilities, may also become an Authorized User for that Participating Organization.

Participating Organizations must also have enforceable agreements with each of its Authorized Users. Agreements may take the form of written policies and procedures of the Participating Organization, so long as such policies and procedures constitute an enforceable agreement with Authorized Users. Participating Organizations must require that all of their Authorized Users comply with applicable laws, clauses in the Participation Agreement directly applicable to Authorized Users, and the WVHIN Policies and Procedures. If an Authorized User is in violation of any of these agreements, the Participating Organization must immediately notify the WVHIN. The WVHIN reserves the right to suspend or terminate user access as necessary.

Authorized Users who are Workforce members of multiple Participating Organizations may have WVHIN Services access rights authorized by each Participating Organization.

A Participating Organization is responsible for informing the WVHIN when the job status or functional role of an Authorized User within its Participating Organization has changed to the extent that would require a role modification or account termination of the Authorized User's account. If access to WVHIN Services is granted through the Participating Organization's electronic health record ("EHR") system, the account administrator for that system must update the Authorized User's access to reflect the change.

If an Authorized User is being terminated, the Participating Organization must inform the WVHIN in a timely manner, and prior to actual termination if possible. This is particularly important if the termination is under less than favorable circumstances. In either case, the WVHIN will disable the Authorized User's account immediately upon termination of employment, unless the Authorized User has access to the account through another Participating Organization where he or she remains rightfully employed or a member of the Workforce. Participating Organizations that grant access to the WVHIN through their EHR must immediately disable access for the terminated Authorized User.

1.4 Training

The WVHIN will make training materials available through its website and may provide other

training opportunities as appropriate. Participating Organizations will be responsible for ensuring their Workforce is trained on the WVHIN Services, the WVHIN Policies and Procedures, and the WVHIN Participation Agreement. If additional training is necessary due to Service updates, the WVHIN will inform Participating Organizations of the changes, and each Participating Organization will then be responsible for notifying its Authorized Users.

1.5 The WVHIN's Rights and Responsibilities

The WVHIN must properly designate a list of Authorized Users from its Workforce in accordance with these Policy and Procedures. In addition, the WVHIN must require any of its Business Associates to properly designate a list of Authorized Users from their respective Workforces in accordance with these Policy and Procedures.

The WVHIN will deny access to its Health Information Exchange to any Business Associate until the WVHIN is in receipt of an executed Business Associate Agreement developed and approved by the WVHIN. Additionally, the WVHIN will deny access to its Health Information Exchange to any Participating Organization until the WVHIN is in receipt of an executed Participation Agreement developed and approved by the WVHIN. The WVHIN will necessarily rely upon the policies and procedures controlling Workforce access made by its Business Associates and Participating Organizations for their Authorized Users.

The WVHIN retains the right to immediately lock out any of its or its Business Associates' Authorized Users who are reported to have violated these Policies and Procedures or any other relevant agreement or policy. This lock out will be terminated after the nature of the violation has been investigated and remedial steps have been taken by the WVHIN and/or the Business Associate to ensure future compliance with these Policies and Procedures.

The WVHIN reserves the right to terminate any individual's status as an Authorized User for good cause, including but not limited to, any fraudulent activity or other activity that constitutes a repeated and ongoing violation or abuse of these Policies and Procedures and/or any other relevant agreement or policy.

2. Authentication of Authorized Users

2.1 Background and Purpose

The purpose of this Section 2 is to describe the process of proving, confirming, and validating that an individual is who he or she claims to be when accessing the WVHIN's Health Information Exchange as an Authorized User. This process is known as authentication.

All Authorized Users must be authenticated prior to accessing Protected Health Information through the WVHIN. The establishment of a functional set of authentication procedures is one important means to minimize the illegitimate access of Protected Health Information by unauthorized individuals.

2.2 User Names and Passwords Generally

The WVHIN web-based portal Services may utilize two-factor authentication, using at least two (2) uniquely known items (e.g., a username and a unique code). The WVHIN and Participating Organizations must ensure that each Authorized User is assigned unique Authentication Information. However, if a Participating Organization provides access to the Health Information Exchange through an in-context or single sign on application to its EHR system, the Authentication Information in use for the EHR will suffice. An Authorized User may not share his or her Authentication Information with any other individual. Each Authorized User is responsible for the activities conducted while logged on to his or her account.

2.3 Password Convention

Passwords will be securely configured. A combination of minimum length, letters (upper and lower case), numbers, and symbols will be required. Passwords will expire at least every ninety (90) days, requiring each user to create a new password at that time. Password history settings will be enforced to ensure that a user does not duplicate a previously used password.

2.4 Lock Outs; Password Resets; Reporting Unauthorized Use

Authorized Users will be able to reset their own passwords set during initial login for the WVHIN Portal or via email for WVDirect accounts. After a limited number of failed log-in attempts, a user will be locked out of the system. Some services will automatically lock a user out of his or her account if it has not been accessed during a limited number of months. In addition, the WVHIN may automatically lock out an Authorized User if he or she has not accessed the WVHIN at any time during the prior 90 days. This lock out will be terminated only after the identity of an Authorized User has been verified, his or her password reset, or other appropriate mitigation measures have been taken.

An Authorized User must immediately report any violation of this Section 2 of these Policies and Procedures, the loss or misuse of Authentication Information, or any other suspicious activity involving an unauthorized individual, to either the Point of Contact or to the WVHIN.

3. Authorized User and Participating Organization Data Access and Use

3.1 Participating Organization's Policy Obligations

All Participating Organizations are required to develop, or have in place, written requirements that govern Participating Organizations' and Authorized Users' access to information systems and use of Protected Health Information. Such policies should be consistent with the permitted purposes set forth in these Policies and Procedures, as well as those set forth in the Participation Agreement, and must be made available to the WVHIN upon request.

3.2 Minimum Necessary; Exceptions to Minimum Necessary

The concept of "Minimum Necessary" is derived from HIPAA and the HIPAA Privacy Rules. Minimum Necessary represents a fundamental and common-sense limitation upon the disclosure of Protected Health Information. In furtherance of the Minimum Necessary rule, Participating Organizations and Authorized Users must only request, use, or disclose the Minimum Necessary amount of information to accomplish the intended purpose of the request, use, or disclosure. Moreover, Authorized Users must only be provided access to the Minimum Necessary amount of data necessary to perform their job function(s) based upon their role and need for such data.

There are a few major exceptions to the Minimum Necessary rule. The most significant exception involves any disclosure to assist in the Treatment of Patients. Hence, the Minimum Necessary rule does not apply to Treatment or Emergency Treatment. The Minimum Necessary rule also does not apply to any disclosure made pursuant to a HIPAA-compliant authorization form signed by the Patient. However, the Minimum Necessary rule does apply to requests, uses, or disclosures of Protected Health Information for Payment, Limited Health Care Operations, and Public Health Reporting.

The WVHIN will develop standard Public Health Reporting protocols designed to disclose only the Minimum Necessary amount of Protected Health Information needed to enable a Participating Organization to comply with its reporting obligations as required or authorized by law. It is the Participant's obligation to ensure the appropriate use of WVHIN Services by Participant and its

Authorized Users.

3.3 Data Misuse

Data available through the WVHIN is to be accessed, viewed, used, and/or disclosed by Participating Organizations and Authorized Users, for Permissible Purposes established by these Policies and Procedures and by the Participation Agreement; provided however, nothing in these Policies and Procedures shall be construed to promote Information Blocking and shall instead be interpreted to permit access, use, and exchange of Protected Health Information or Electronic Health Information to the extent permitted by applicable law.

The WVHIN uses a privacy tool for additional monitoring of all user activities associated with data access to ensure all provisioned accounts are being used appropriately; however, it is ultimately the Participating Organization's obligation to ensure the appropriate use of WVHIN Services by Participating Organization and its Authorized Users. Any misuse of data available through the WVHIN is to be reported to the WVHIN as soon as discovered. Data misuse will be investigated and verified. The WVHIN will notify all impacted Participating Organizations at the conclusion of such investigations, if it is determined that a misuse of data has occurred. Upon identification of a potential misuse of data, the WVHIN shall notify the Participating Organization's Point of Contact and Privacy Officer. Participating Organizations shall cooperate and respond timely to WVHIN requests for information concerning the data misuse. Upon request by the WVHIN, the responsible Participating Organization may be required to notify Patients. If appropriate, the WVHIN will also take actions necessary to remedy the misuse of data. These actions may include, but are not limited to, suspension and/or termination of the status of a Participating Organization or Authorized User(s). Each instance of misuse will be considered a "security incident" and will be investigated as a potential Breach under the HIPAA Security Rules.

The WVHIN reserves the right to terminate any Participating Organization's status or Authorized User's status for good cause, including but not limited to, any fraudulent activity or other activity that constitutes a repeated and ongoing violation or abuse of these Policies and Procedures, the Participation Agreement, and/or any other relevant agreement or policy.

3.4 Discipline for Non-Compliance

Each Participating Organization must implement procedures to mitigate and deter the misuse of data and issue appropriate discipline to hold its Authorized Users responsible for misuse of data obtained through the WVHIN. Applicable procedures in place for use of other health information systems may be leveraged for misuse of data.

4. Patient Access and Rights

4.1 Patient's Right of Access to Data

Available Information and Methods for Access

Patients will have access to their data shared through the WVHIN's Health Information Exchange (HIE) in accordance with applicable laws and regulations. This data includes, but is not limited to, clinical and encounter data that constitutes electronic Protected Health Information or Electronic Health Information (collectively, "Patient Data"). The WVHIN will update methods for Patient access on its website. Additionally, WVHIN will make available educational materials about best practices and methods for Patients accessing their Patient Data. In addition, the materials will remind patients that the WVHIN maintains only summary Patient Data, and not the complete medical record. Thus, Health Care Providers and/or Health Plans (as applicable) will likely have more robust and comprehensive medical record information, and may be the most appropriate

contact if Patients have questions or concerns about their data. The WVHIN Customer Care Team will answer Patient questions about how to access Patient Data, but patients who have questions about their data will be directed to the health care provider or Health Plan (as applicable) who shared the information.

All requests for access to Patient Data shall be reviewed in accordance with Section 5.8 Uses and Disclosures to Non-Participant Third-Parties as set forth in these Policies and Procedures.

4.2 Patient's Right to Accounting of Disclosures

Upon receipt of a request from a Patient, Participating Organizations are required by the HIPAA Privacy Rules to make available an accounting of certain disclosures of the Patient's Protected Health Information. The accounting applies to disclosures of paper and electronic Protected Health Information up to a period of seven (7) years prior to the date of the request. An accounting provided by a Participating Organization must include disclosures to and by its Business Associates. Participating Organizations make the determination whether to disclose Protected Health Information and log the disclosure if required to do so under the HIPAA Privacy Rules, the HITECH Act, and their implementing regulations. As such, the Participating Organization whose accounting of disclosures is being sought by a Patient is the only organization that can logically evaluate and provide for a full accounting of the Patient's Protected Health Information disclosures. Therefore, any request for an accounting must be directed to the Participating Organization(s) retaining Patient Protected Health Information for the Participating Organization to fully evaluate the request and a suitable response to the request.

If a Participating Organization deems it necessary, the WVHIN shall make available to the Participating Organization information about the Health Information Exchange's disclosures of Protected Health Information, if any, that must be included to fully and properly respond to the Patient's request for accounting. The WVHIN shall be obligated to provide an accounting of only those disclosures made through the Health Information Exchange within the following time periods:

(i) If the disclosure is from one Participating Organization to another Participating Organization for Treatment, Payment, or Health Care Operations, the accounting must include only those disclosures made during the three (3) year period immediately preceding the date of the Patient's request.

(ii) If the disclosure is from the WVHIN to another party for Public Health Reporting or any other purpose permitted by the WVHIN Policies and Procedures, the accounting must include only those disclosures made during the six (6) year period immediately preceding the date of the Patient's request, or the period during which the Participating Organization has had connectivity with the WVHIN immediately preceding the date of the Patient's request, whichever is shorter.

The WVHIN shall respond to a Participating Organization's request for an accounting within 30 days of the WVHIN's receipt of the request. For each disclosure for which an accounting must be provided, the WVHIN's response shall include all information the WVHIN is obligated to track pursuant to applicable laws, including but not limited to the HIPAA Privacy Rules and the HITECH Act.

4.3 Patient Notice, Patient Consent, and Opt-Out Rights

The WVHIN will offer Patients a meaningful way to decide whether to participate or not participate in the Health Information Exchange that it sponsors. The default Patient Consent model for the Query-based Health Information Exchange is Opt-Out. A Patient who does not want to participate in the Query-based exchange must take specific action to Opt-Out. This means that all Patients of

a Participating Organization will be automatically enrolled in the WVHIN's Health Information Exchange, and no affirmative action needs to be taken by a Patient to establish his or her Consent. A Patient shall be deemed to have given his or her Consent to participate until and unless the Patient affirmatively Opts-Out of the WVHIN's Health Information Exchange.

If a Patient does not Opt-Out of the WVHIN's Health Information Exchange, his or her Protected Health Information will generally be disclosed in response to a specific request, or Query, made by a Participating Organization for a Permissible Purpose. However, a Patient's Protected Health Information will not be disclosed in response to such a Query when it contains Sensitive Health Information for which a specific authorization is required even if a Patient does not Opt-Out (see Section 8 of these Policies and Procedures for more information about Sensitive Health Information and disclosures of such information); provided that the WVHIN may disclose Sensitive Health Information to the extent a valid Patient authorization is executed and maintained.

For a Patient who has Opted-Out of the Health Information Exchange, the WVHIN will ensure that no Protected Health Information will be disclosed except for the Permissible Purpose of Public Health Reporting. Instead, the Participating Organization that submitted the Query will receive a message that the Patient has Opted-Out of the WVHIN's Health Information Exchange. All decisions made by a Patient to Opt-Out of the Health Information Exchange will be electronically recorded in the WVHIN's Health Information Exchange to ensure compliance with each Patient's decision to Opt-Out. The Patient Opt-Out election shall also apply to other national, regional, and proprietary networks with whom the WVHIN may contract to the extent feasible given the technological structure of the external networks.

A Participating Organization shall not deny care to any Patient solely because he or she elects to Opt-Out of the Health Information Exchange.

Opt-Out applies to Query-based transactions only and does not apply to automatic message delivery from a data source to a physician of record or point-to-point secure messaging. For example, if a primary care physician orders a lab from a national lab, the result for that order will still be electronically delivered to the ordering Health Care Provider. If a Patient Opts-Out, the result will not be available to other Participants who Query the exchange.

To ensure that Patients can make an informed choice, each Patient will receive a Patient Notice from his or her Participating Organization prior to or during the first Patient encounter after the Participating Organization enrolls in the WVHIN's Health Information Exchange. In the case of a Health Plan, the Patient Notice shall be provided during the Patient's initial enrollment or during the next annual mailing to Patients then covered by the Health Plan. The Patient Notice is available on the WVHIN website, www.wvhin.org, and explains the function of the Health Information Exchange. Participating Organizations may incorporate the WVHIN Patient Notice within their notice of privacy practices. Participating Organizations must be able to educate Patients on the functionality and purpose of the WVHIN and the Opt-Out process as needed.

Patients may Opt-Out by completing a paper form and mailing, emailing, or faxing it to the WVHIN, calling a toll-free number, or submitting the form on-line. Upon receipt of the Opt-Out request, there will be a period of one (1) business day before the Opt-Out is recorded in the WVHIN's system, meaning that Patient data may be available for Query during this interim time after the Opt-Out request has been submitted.

A Patient may choose to Opt-Out at any time, even after having already been enrolled in the Health Information Exchange. However, any exchange of Protected Health Information that may have occurred prior to a Patient's decision to Opt-Out will not be reversed. Patients may opt back into the Health Information Exchange at any time by calling the WVHIN Customer Care Team at 1-844-468-5755.

4.4 Patient's Right to Amend Protected Health Information

The HIPAA Privacy Rules establish a process by which Patients may seek to amend their own Protected Health Information. This right of amendment applies to any Designated Record Set maintained by a Covered Entity, including a Health Care Provider, Health Plan, or Health Care Clearinghouse.

The WVHIN is neither a Covered Entity nor a licensed, certified, or registered Health Care Provider. Moreover, it is not contemplated that the WVHIN will act as a depository of a Designated Record Set containing Protected Health Information for or on behalf of any of its Participating Organizations, but will instead facilitate the exchange of Protected Health Information between Participating Organizations for one or more Permissible Purposes. Participating Organizations are the originators of the Protected Health Information, and maintain the Designated Record Sets in which this information resides. As such, the Participating Organization whose Designated Record Set is subject to the Patient's request for amendment is the only organization that can logically evaluate such requests.

Accordingly, if a Patient makes a request to the WVHIN to amend his or her Protected Health Information, it must be directed in writing to the applicable Participating Organization(s). The Participating Organization(s) will be solely responsible for making all determinations regarding the grant or denial of the requested amendment, and for ultimately providing for the amendment with respect to its own Designated Record Set.

4.5 Patient's Right to Request Restrictions on the Use or Disclosure of Own Protected Health Information

The HIPAA Privacy Rules establish a process by which Patients may request restrictions on the use and disclosure of their own Protected Health Information to a Covered Entity. This right to request restrictions applies to uses and disclosures of the Patient's Protected Health Information for Treatment, Payment, and Limited Health Care Operations.

Generally, a Covered Entity is under no obligation to agree to requests for restrictions; however, the Covered Entity is required to have policies in place establishing a procedure to accept or deny such requests. The requested restrictions may either be accepted or denied by the Covered Entity whose records are subject to the Patient's request. A Covered Entity that accepts the request must comply with the restrictions, except for the purpose of providing the Patient with Emergency Treatment. If certain requirements are met, a Covered Entity is required to accept a Patient's restriction request. Out-of-Pocket Goods and Services is the only required restriction.

The WVHIN is not a Covered Entity and therefore will not accept requests for restrictions on the use and disclosure of Patient Protected Health Information for or on behalf of any of its Participating Organizations. The goal of the WVHIN is to facilitate exchange of Protected Health Information between Participating Organizations for one or more Permissible Purposes. Participating Organizations are the originators of the Protected Health Information and maintain the Patient records in which this information resides. As such, the Participating Organization whose records are subject to the Patient's request for restrictions is the only organization that can logically evaluate the request.

Patient-Restricted Information is considered Sensitive Health Information (see Section 8 of these Policies and Procedures for more details on Sensitive Health Information).

If a Patient makes a request in writing to the WVHIN to restrict the use or disclosure of his or her Protected Health Information, the WVHIN will forward that request to the applicable Participating Organization(s). The Participating Organization(s) will be solely responsible for making all determinations regarding the acceptance or denial of the requested restriction, and for

electronically tagging the restricted information as Sensitive Health Information.

5. Permissible Purposes

5.1 Background; Permissible Purposes Generally

One of the fundamental principles identified by the Office of the National Coordinator for Health Information Technology is the need for appropriate limits on the collection, use, and disclosure of Protected Health Information by a Health Information Exchange organization such as the WVHIN. The WVHIN therefore must establish parameters on Participating Organizations to ensure that Protected Health Information will only be disclosed for a Permissible Purpose. The placement of appropriate limits upon the Health Information Exchange through the definition of what constitutes a Permissible Purpose will enhance Patient confidence in the exchange process, and will minimize the potential for misuse or abuse of Protected Health Information.

Any disclosure of Protected Health Information for a Permissible Purpose must be conducted in compliance with federal and state laws. Authorized Users may access and use data through the WVHIN for the following Permissible Purposes:

- ► Treatment;
- ► Emergency Treatment;
- ► Payment;
- ► Limited Health Care Operations;
- ► Public Health Reporting; and
- ► Public Health Use Cases.

The scope of each of these Permissible Purposes under the WVHIN's Health Information Exchange is further described below.

5.2 Permissible Purpose of Treatment

The Permissible Purpose of Treatment allows the exchange of Protected Health Information from one Participating Organization through the Health Information Exchange to another Participating Organization. Treatment means the provision of health care items or services to a Patient, and shall have the same meaning as under the HIPAA Privacy Rules. The provision of health care items or services may include direct Patient care as well as the consultation, coordination, management, or referral of a Patient between or from one Participating Organization to another. 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).

5.3 Permissible Purpose of Emergency Treatment

The Permissible Purpose of Emergency Treatment allows the exchange of Protected Health Information from one Participating Organization through the Health Information Exchange to another Participating Organization. Emergency Treatment means the provision health care items or services to a Patient suffering from a condition which poses an immediate threat to the health of the Patient (for example, death or serious impairment to one or more bodily systems, organs, or parts), and which requires immediate medical intervention. Emergency Treatment is a distinct subset of Treatment, although it is sometimes made subject to differing Policies and Procedures by the WVHIN.

5.4 Permissible Purpose of Payment

The Permissible Purpose of Payment allows the exchange of Protected Health Information

between Participating Organizations for Payment-related activities which relate to the Patient who is the subject of the disclosure or use. “Payment” shall have the same meaning as set forth under the HIPAA Privacy Rules. Payment is defined under HIPAA as any activity undertaken by a Health Care Provider or Health Plan to obtain or provide reimbursement for the provision of health care to a Patient.

The exchange of Protected Health Information related to Payment must contain only the Minimum Necessary amount of Protected Health Information as is required or authorized for the specific requested Payment purpose.

A Patient may pay in full for goods and services received from a Participating Organization, and request the Participating Organization not to disclose such information to a Health Plan for Payment purposes. Such information will constitute Out-of-Pocket Goods and Services, and will be considered Patient Restricted Information – and as a corollary – will also constitute Sensitive Health Information (as further detailed in Section 8 of these Policies and Procedures). The Participating Organization will cooperate with the WVHIN to electronically tag all Out-Of-Pocket Goods and Services to block them from being disclosed through the Health Information Exchange for Payment purposes in compliance with the Sensitive Health Information section (Section 8) of these Policies and Procedures.

Likewise, a Patient may request a Participating Organization to restrict the disclosure of Protected Health Information for a Payment purpose. If granted, such information will constitute Patient-Restricted Information and Sensitive Health Information. A Participating Organization shall cooperate with the WVHIN to electronically tag all Patient-Restricted Information (if it has agreed to a Payment restriction) to block it from being disclosed through the Health Information Exchange for Payment purposes in compliance with the Sensitive Health Information section (Section 8) of these Policies and Procedures.

The WVHIN will not disclose any Protected Health Information to consumer reporting agencies for Payment purposes.

5.5 Permissible Purpose of Limited Health Care Operations

The Permissible Purpose of Limited Health Care Operations allows the exchange of Protected Health Information between Participating Organizations for certain Health Care Operations of a Participating Organization if: (a) the Participating Organization submitting the Inquiry has or had a Treatment or Payment relationship with the Patient whose Protected Health Information is being requested, (b) the Protected Health Information pertains to such relationship, and (c) the purpose of the use or disclosure is listed in paragraph (1) or (2) of the definition of Health Care Operations under the HIPAA Privacy Rules or is for the purpose of health care fraud and abuse detection or compliance.

The exchange of Protected Health Information for Limited Health Care Operations must contain only the Minimum Necessary amount of Protected Health Information as is required or authorized for the specific requested Limited Health Care Operations purpose.

It is important to reiterate that HIPAA does not authorize the disclosure of Protected Health Information for all types of Health Care Operations included within the HIPAA Privacy Rules. Rather, disclosure without Patient Authorization may occur only for those health care improvement and quality enhancement purposes in paragraph (1) and (2) of the definition, or for the purpose of health care fraud and abuse detection or compliance.

For the purposes of the Health Information Exchange, “Limited Health Care Operations” specifically includes quality assessment and improvement activities (including utilization review), outcomes evaluation, development of clinical guidelines, population-based activities relating to

improving health and reducing health care costs, protocol development, case management and care coordination, and contacting Health Care Providers and Patients with information about Treatment alternatives.

All Participating Organizations are specifically prohibited from seeking access to Protected Health Information through the Health Information Exchange for non-authorized Health Care Operations as set forth in paragraphs (3), (4), (5), and (6) of the definition contained in the HIPAA Privacy Rules. Such non-authorized Health Care Operations include, but are not limited to, underwriting purposes, premium ratings, legal services, business planning, business management, general administrative services, grievance resolution, due diligence, and fundraising. All Participating Organizations are also specifically prohibited from seeking access to Protected Health Information through the Health Information Exchange for the purpose of a Health Plan sponsor's employment-related actions or decisions, or in connection with any other benefit or employee benefit plan of a Health Plan sponsor. Likewise, the WVHIN is prohibited from using, disclosing, or selling Protected Health Information for marketing or other commercial purposes, or for any other non-authorized Health Care Operations.

5.6 Permissible Purpose of Public Health Reporting

The Permissible Purpose of Public Health Reporting allows the exchange of Protected Health Information through the WVHIN to a federal or state agency for the reporting and surveillance of specified diseases and health conditions as required or authorized by law, electronic lab reporting as required or authorized by law, and for the reporting of immunization data. Public Health Reporting shall contain the minimum amount of Protected Health Information or Personal Demographic Information required or authorized for the reporting purpose. A Patient may not Opt-Out of Public Health Reporting. *See* Section 4.3 of the Policies and Procedures.

5.7 Modification of Permissible Purposes; Public Health Use Cases

To the extent consistent with applicable laws and regulations, Permissible Purposes may be modified or added with the approval of the WVHIN Board of Directors, and such modifications or additions will be treated as amendments to the Permitted Purposes and posted on the WVHIN website.

With the approval of the WVHIN Board of Directors, Public Health Use Cases may be extended to entities that are Covered Entities or are public health agencies. Upon a finding that such an extension is in furtherance of the mission of the WVHIN, the Covered Entity or public health agency will be required to enter into a written agreement with the WVHIN. The agreement will protect the interests of the WVHIN and its Participating Organizations by assuring the integrity of the WVHIN Services and the appropriate use of the information to be provided to the Covered Entity or public health agency.

5.8 Uses and Disclosures by Non-Participant Third Parties

The WVHIN may receive requests to access, use, and disclose Protected Health Information or Electronic Health Information from non-participant third parties. For example, a treating health care provider that is not a WVHIN Participant may request access to data through the WVHIN for Treatment purposes. Patients are considered non-participant third parties and may also request access to Patient Data as set forth in Section 4.1. The WVHIN will establish functional authentication procedures in order to authenticate such requests.

Such requests will be considered on a case-by-case basis in a manner that avoids any Information Blocking prohibition. Requests from non-participant third parties shall be evaluated in accordance with applicable laws and organizational policy, to the extent applicable, to

determine whether any requested access, use, or disclosure meets one of the following Information Blocking exceptions:

(i) Presents a danger to the life or physical safety or a substantial risk of harm to a Patient or other person;
(ii) Improperly violates Patient Privacy;
(iii) Presents a significant risk of security to Electronic Health Information;
(iv) Would be infeasible to fulfill;
(v) Interferes with reasonable HIE maintenance or improvement activities;
(vi) Cannot technically be fulfilled in the manner requested;
(vii) Requires imposition of a reasonable, cost-based fee before fulfillment;
(viii) Would violate reasonable and non-discriminatory licensing requirements; or
(ix) Permits limitation on the manner in which Electronic Health Information is shared to only via the Trusted Exchange Framework and Common Agreement ("TEFCA").

The above factors will be evaluated by the WVHIN in accordance with applicable law and regulations, as well as any WVHIN organizational policies.

The WVHIN may charge fees to non-Participant third parties in fulfilling requests to access, use, and disclose Protected Health Information or Electronic Health Information. Fees shall be consistent with the costs incurred in fulfilling the request in the content and manner requested, as permitted by applicable law.

The WVHIN offers methods by which providers may document and provide notice of a determination of danger to life or physical safety or a substantial risk of harm to a Patient or other person, as may be applicable, that would otherwise arise from the access, exchange or use of certain Electronic Health Information. The WVHIN shall limit access to Electronic Health Information under Information Blocking's Preventing Harm exception referenced above at (i), if a provider, who has or had a clinician-patient relationship with the Patient, electronically submits a risk of harm determination via the WVHIN's Prevention of Harm tool in accordance with applicable law. The WVHIN shall not block Electronic Health Information in any manner broader than necessary. The risk of harm must either be determined by a provider or arise from data as permitted by the Prevention of Harm exception. No other type of risk of harm qualifies for purposes of WVHIN Policies and Procedures. If the risk of harm does not arise from data or is not determined by a provider, in accordance with Information Blocking's Preventing Harm exception, the WVHIN shall not block access to Electronic Health Information unless otherwise required by law to do so, or another Information Blocking exception applies. The WVHIN may only act to withhold Electronic Health Information in accordance with risk of harm determinations submitted via the WVHIN's Prevention of Harm tool or an alternative electronic method agreed to by the WVHIN. The WVHIN will honor provider determinations until such time as it becomes aware that the determination is revoked. Any such revocation must be submitted in writing to PrivacyOfficer@crisphealth.org, or such other alternative electronic methods as agreed to by the WVHIN.

5.9 Deidentified Data

The WVHIN may Deidentify Protected Health Information, and may disclose or use Deidentified data for any public health or research purpose permitted by applicable law and approved by the WVHIN Board of Directors. Deidentification will meet the requirements of the HIPAA Privacy Rules, and any interpretation thereof carrying the force of law. Requests for Deidentified data must be submitted to the WVHIN in writing, and must specify in detail the legitimate public health or research purpose for which the Deidentified data is sought. The WVHIN shall have complete discretion in evaluating any request for Deidentified data, and may deny a request for Deidentified data for any reason. Any requestor approved to obtain Deidentified data from the WVHIN must strictly limit its use in accordance with a data use agreement approved by the WVHIN. The requestor may not re-use the Deidentified data for another purpose or disclose the Deidentified

data to any third party without the express written consent and approval of the WVHIN. The WVHIN, through its Workforce or Business Associates, may access Protected Health Information through the Health Information Exchange to create Deidentified data in accordance with this Section 5.9.

6. Business Associates and Business Associate Agreements

6.1 Business Associates; Business Associate Subcontractors

A Business Associate is defined as a person or entity that performs a function, activity, or service on behalf of a Participating Organization or another Business Associate involving the disclosure of Protected Health Information to the Business Associate. The WVHIN is a Business Associate to each of its Participating Organizations. Subcontractors and vendors to the WVHIN may be Business Associate Subcontractors of the WVHIN. A Business Associate shall have the same meaning as such term is defined in the HIPAA Privacy Rules. Likewise, WVHIN Business Associate Subcontractors shall fully comply with the requirements of the HIPAA Privacy Rules, the HIPAA Security Rules, and the HITECH Act, as implemented by regulation, and may not further use or disclose Protected Health Information other than as permitted or required by any Business Associate Agreement entered into with the WVHIN, or as required by law.

A Business Associate Agreement is a formal written contract between the WVHIN and Participating Organizations or WVHIN Business Associate Subcontractors, which obligates the WVHIN and its Business Associate Subcontractors to maintain the privacy and security of Protected Health Information in accordance with the requirements of the HIPAA Privacy and Security Rules. The WVHIN will enter into written Business Associate Agreements with Participating Organizations and WVHIN Business Associate Subcontractors.

Operation or management of the Health Information Exchange may require the access, use, or disclosure of Protected Health Information by the WVHIN, or its Business Associate Subcontractors to perform functions or activities on behalf of Participating Organizations. A Business Associate is obligated not to access, use, or further disclose Protected Health Information other than as permitted or required by the Business Associate Agreement or as required by law.

6.2 Business Associate Agreements

Each Participating Organization must enter into a Business Associate Agreement with the WVHIN prior to obtaining authorization to access, use, or disclose Protected Health Information through the Health Information Exchange. Should either the WVHIN or a Participating Organization elect to terminate their Business Associate Agreement for any reason, the Participating Organization must no longer be allowed to access the WVHIN's Health Information Exchange. The Business Associate Agreement between the WVHIN and each of its Participating Organizations must comply fully with all of the requirements of the HIPAA Privacy Rules, the HIPAA Security Rules, and the HITECH Act, as implemented by regulation, and other applicable laws.

Likewise, the WVHIN must enter into a Business Associate Agreement with each of its Business Associate Subcontractors prior to authorizing the latter to perform any services on behalf of the WVHIN that could cause the Business Associate Subcontractor to receive, maintain, transmit, or create Protected Health Information from or through the WVHIN's Health Information Exchange. The WVHIN and its Business Associate Subcontractors may access, use, or disclose only the Minimum Necessary Protected Health Information obtained from or on behalf of any Participating Organization for the following purposes:

(i) For purposes of installing, testing, maintaining, or operating the Health Information Exchange;

(ii) In order to provide technical, administrative, and maintenance support to Participating Organizations in the use of the Health Information Exchange;

(iii) In order to provide training to Workforce members, to Participating Organizations and their Authorized Users, and to WVHIN Business Associate Subcontractors and their Workforce members;

(iv) For purposes of the WVHIN's appropriate management and administration; and

(v) To perform any other service or function reasonably necessary to carry out the mission of the WVHIN as defined in its authorizing statute and rules.

7. Data Contributor Responsibilities

7.1 Testing and Validation

Participating Organizations who submit data to the WVHIN (collectively referred to as "Data Contributors") must complete testing prior to going live with connectivity to the WVHIN. In addition to initial testing, Data Contributors are responsible for validating data on a test platform provided through the WVHIN when changes or upgrades to their source systems are made. Data Contributors should notify the WVHIN prior to system changes or upgrades in order to allow sufficient time for testing. Data validation will be completed by comparing the data in WVHIN's system to that in the Data Contributor's source system.

The WVHIN may provide guidance pertaining to testing, but it is the Data Contributor's responsibility to execute a complete test plan in accordance with its own testing policies and procedures. Following successful completion of testing, Data Contributors must confirm that they are ready to go-live.

7.2 Data Availability

Data Contributors will make appropriate data available to the WVHIN consistent with the Services offered by the WVHIN. For example, the WVHIN is initially focused on receiving Admit Discharge Transfer ("ADT"), laboratory reports, radiology reports, and a subset of electronic documents including discharge summaries, consultations, history and physicals, operative notes, as well as other data types that may be deemed appropriate in the future. For each Data Contributor, information made available to the WVHIN Services will be subject to appropriateness and technical readiness. For a Data Contributor to be connected to and remain connected to the WVHIN, it must submit at least one (1) defined data type. Contribution of data must occur over a secure connection configured by the WVHIN and the Data Contributor in conformance with the HIPAA Security Rules and all other applicable laws, regulations, and policies.

8. Sensitive Health Information

8.1 Background and Purpose

Participating Organizations who submit data to the WVHIN must refrain from sending certain Sensitive Health Information that is restricted from disclosure for certain purposes by local, state, district, and federal law. Depending upon the Permissible Purpose for which Sensitive Health Information is being sought, the law may require a Patient to specifically authorize in writing a disclosure of his or her Sensitive Health Information by signing a document that satisfies all legal requirements for the disclosure. Sensitive Health Information that requires the execution of a specific written consent or authorization shall not be disclosed through the WVHIN's Health Information Exchange unless a WVHIN compliant consent or authorization management process

is registered. Participating Organizations are responsible for complying with applicable laws and for filtering any information that should not be disclosed via the WVHIN Services. Each Participating Organization is responsible for determining which data to contribute to the WVHIN Services and which data to withhold. By disclosing data to the WVHIN, Participating Organizations authorize the further access, exchange, and disclosure of the data to other Participating Organizations and other individuals or third parties legally permitted to access such data via the WVHIN's Health Information Exchange.

Any Participating Organization that receives Sensitive Health Information in response to an Inquiry must refrain from re-disclosing such information to third parties except as may be authorized by law.

Sensitive Health Information categories include, but may not be limited to:

- ► Substance Use Disorder Information;
- ► Psychotherapy Notes;
- ► Out-Of-Pocket Goods and Services; and
- ► Patient-Restricted Information.

The scope of each of these categories of Sensitive Health Information is further described below.

8.2 Substance Use Disorder Information

Substance Use Disorder Information means any information that is defined as confidential and protected by federal law pursuant to 42 C.F.R. Part 2. Substance Use Disorder Information is considered Sensitive Health Information. It includes any information from a federally assisted Part 2 program, as defined by federal regulation in 42 C.F.R. Part 2, which would identify the Patient as having a substance use disorder. In the absence of a written consent signed by the Patient, federal law permits Substance Use Disorder Information to be disclosed for only the Permissible Purpose of Emergency Treatment, for federally-regulated research purposes, or for audit and evaluation activities related to Payment. Under the WVHIN's current technological configuration, Substance Use Disorder Information may only be shared through the WVHIN's Health Information Exchange pursuant to a valid consent executed by the Patient. This consent will be registered and available through the WVHIN in summary explanation form. Substance Use Disorder Information associated with a registered consent may be exchanged for the Permissible Purposes of Treatment, Payment (other than audit and evaluation), or Limited Health Care Operations. Any disclosure of Substance Use Disorder Information pursuant to Patient consent or other authorization shall be accompanied by a written notice in accordance with applicable law. The Patient consent shall be in accordance with applicable laws governing Substance Use Disorder Information.

The WVHIN may act as a Qualified Service Organization to a Part 2 program, and may thereby obtain access to Substance Use Disorder Information to assist the Part 2 program in its own Treatment activities. When doing so, the WVHIN must enter into a Qualified Service Organization Agreement ("QSOA") with the Part 2 program governing the WVHIN's permissible uses and disclosures of Substance Use Disorder Information that is compliant with all Part 2 requirements.

8.3 Psychotherapy Notes

Psychotherapy Notes are considered Sensitive Health Information. The HIPAA Privacy Rule establishes the confidential nature of Psychotherapy Notes, which are defined under HIPAA as notes recorded by a mental health provider documenting or analyzing the contents of a conversation during a private, group, or family counseling session and that are separated from the rest of the Patient's medical record. *See* 45 C.F.R. § 164.501. Psychotherapy Notes exclude any

summary of notes regarding: diagnosis, functional status, treatment plans, symptoms, prognosis, progress to date, medication prescription and monitoring, counseling sessions start and stop times, the modalities and frequencies of Treatment furnished, and the results of clinical tests. In the absence of a specific written authorization signed by the Patient applicable only to Psychotherapy Notes, federal law prohibits the disclosure of Psychotherapy Notes for any Permissible Purpose except Public Health Reporting. Psychotherapy Notes may only be shared for Treatment, Emergency Treatment, Payment, or Limited Health Care Operations if there is a Patient's specific signed consent or authorization on a currently valid document that satisfies all legal requirements for the disclosure.

8.4 Out-Of-Pocket Goods and Services

Out-Of-Pocket Goods and Services are considered Sensitive Health Information. They include any goods or 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 said goods and services to a Health Plan as contemplated under the HIPAA Privacy Rules. In the absence of a written authorization signed by the Patient applicable to Out-Of-Pocket Goods and Services, federal law permits Out-Of-Pocket Goods and Services to be disclosed for any Permissible Purpose to any entity other than a Health Plan. Out-of-Pocket Goods and Services may be shared with a Health Plan only if there is a Patient's signed consent or authorization on a currently valid document that satisfies all legal requirements for the disclosure.

8.5 Patient-Restricted Information

Patient-Restricted Information is considered Sensitive Health Information. It includes any information that is subject to a disclosure restriction impacting any Permissible Purpose, other than Public Health Reporting and Emergency Treatment, and that has been specifically requested by a Patient and agreed to by the Participating Organization as contemplated under the HIPAA Privacy Rules and other applicable laws. In the absence of a specific written authorization signed by the Patient, federal law permits the disclosure of Patient-Restricted Information as defined herein for the Permissible Purposes of Emergency Treatment and Public Health Reporting. Patient-Restricted Information may only be shared for Treatment, Payment, and Limited Health Care Operations if it does not include a restriction for such purposes or if there is a Patient's signed consent or authorization on a currently valid document that satisfies all legal requirements for the disclosure.

9. Interstate Data Exchange

9.1 National Networks

One of the main goals of WVHIN is to ensure that health data is accessible for clinicians and patients to make the best decisions, no matter where in the states and territories of the United States a patient receives care. Therefore, the WVHIN may participate in several national networks. National networks electronically connect Health Information Exchanges (HIEs) and more localized Health Information Networks (HINs) throughout the country. They also provide a common framework for technology and standards for privacy and security. Each national network has its own governing body, rules, and legal agreements, but they all conceptually operate in the same manner.

The WVHIN currently participates in the following national networks:

- The eHealth Exchange network;
- The CommonWell network; and
- The Carequality interoperability framework.

Each of these networks and frameworks has its own governing body, rules, and legal agreements. Currently, the WVHIN only shares data with the above reference national networks for the Permissible Purpose of Treatment.

9.2 TEFCA

TEFCA is a government-endorsed framework for the nationwide exchange of health information that is intended to further connect existing national networks. A goal of TEFCA is to ensure all national networks are connected to eliminate the need to connect to multiple networks. To the extent the WVHIN elects to participate in TEFCA it will do so through the eHealth Exchange network. Participating Organizations will be able to participate in TEFCA through the WVHIN, if they choose to do so, by executing an addendum to the WVHIN Participation Agreement.
Similar to the WVHIN and national networks, TEFCA has its own governing body, rules, and legal agreements. More information on WVHIN's planned participation in TEFCA may be found on the WVHIN's website.

10. Data Controls

10.1 Privacy and Security

Participating Organizations are responsible for maintaining sufficient safeguards and procedures, in compliance with all applicable provisions of federal and state law, including HIPAA, the HITECH Act, and the HIPAA Privacy and Security Rules set forth in 45 C.F.R. Parts 160 and 164, as may be amended, to preserve the security and privacy of Protected Health Information. The Participant is responsible for maintaining appropriate administrative, physical, and technical safeguards to prevent unauthorized use or disclosure of Protected Health Information according to HIPAA standards. Participants are responsible for ensuring their processes and practices are in compliance with the HIPAA Privacy Rules and the HIPAA Security Rules.

10.2 Data Consumption

Participating Organizations can contribute and/or consume data either via the WVHIN Services or through their EHR systems. The hardware and software requirements for connecting to the WVHIN Services depends on the means a Participating Organization is using to contribute and consume data, but in any event such hardware and software shall be capable of facilitating a secure and appropriate transmission of data.

10.3 Data Retention

The WVHIN will retain disclosure data for a minimum period of seven (7) years in order to maintain an auditable history of each transaction through the WVHIN Services. In addition, the WVHIN will retain copies of all its policies and procedures, all complaints received and resolved by the WVHIN, all Breach and potential Breach investigations undertaken by the WVHIN, all agreements with Participants, Business Associates, and other third-parties, as well as any other administrative, business, or financial records of the WVHIN for a minimum period of seven (7) years.

The WVHIN may allow access or otherwise release data for Public Health Reporting or in other civil, criminal, or crisis-related matters where compelled to provide that data by a lawful order. Each request for data from external organizations will be independently vetted to ensure the request is legal and appropriate. The WVHIN will not release any Protected Health Information to anyone for commercial, private, or other reasons that are not related to Treatment or Emergency Treatment, Payment, Limited Health Care Operations, or other Public Health Reporting purpose and other purposes as may be adopted and added as a Permissible Purpose from time to time.

10.4 Return of Data

If a Participating Organization wishes to terminate access to the WVHIN Services, the WVHIN will disable that Participating Organization's data feeds and terminate the Participating Organization's ability to access the WVHIN Services. All data that has been incorporated into a Participating Organization's EHR system prior to a Participating Organization's termination will continue to be the property of that Participating Organization. Additionally, the WVHIN or the terminating Participating Organization may retain one copy of the other's Proprietary Information to the extent reasonably necessary to document matters relating to the Participation Agreement for legal or insurance reasons or for similar purposes, provided that the restrictions on Proprietary Information in the Participation Agreement continue to apply to the retained copy.

11. Systems Operations and Services

11.1 Hardware and Software

The WVHIN contracts with certain third-parties to provide the WVHIN Services. In turn, the third-party purchases Health Information Exchange infrastructure components and licenses from vendors as commercial off the shelf applications ("COTS"). The WVHIN Services are hosted in a distributed environment to allow for redundancy and reliability. Through the vendor's framework, the WVHIN makes available services (the "WVHIN Services") to its Participants for data consumption.

11.2 Availability and Network Monitoring

The WVHIN Services are monitored 24x7x365 by the WVHIN and/or third parties. The WVHIN utilizes a hosted services agreement to facilitate uptime that is consistent with industry standards for a Health Information Exchange, not including scheduled downtime. For each calendar year, scheduled hardware, software, and communications maintenance shall not exceed an average of eight (8) hours in total per calendar month. All scheduled maintenance will be carried out on dates and at times by an authorized third party with at least three (3) business days' notice provided to all Participating Organizations via e-mail or other comparable electronic method (such as the WVHIN or third-party website).

In the event of unexpected downtime, Participating Organizations will be electronically notified between four (4) hours and three (3) business days after discovery of the problem, depending on the severity level. Until notice of resolution, update frequency will occur every eight (8) business hours to every three (3) business days, depending on the severity level.

11.3 Maintenance

Participating Organization support staff will be expected to assist with issues surrounding on-going training, Master Patient Index ("MPI") administration, data availability, data quality, system upgrades and downtime, and privacy and security issues. The Point of Contact will be responsible for the maintenance of Authorized User profiles and will be required to verify Authorized Users, at a minimum, every 90 days. This includes providing all necessary information to the WVHIN for adding users, deleting users, and assigning or changing user roles. The Point of Contact must notify the WVHIN immediately if a user's employment or Workforce status at the organization has been terminated or if his or her functional role has changed. This notification can be done either using the self-services HIE Admin Tool (recommended) or an email to wvhinsupport@crisphealth.org. The Point of Contact will also be responsible for checking that Authorized Users have completed all necessary policy training prior to obtaining access to the WVHIN Services, and for monitoring the general use and operations of the WVHIN Services.

12. Help Desk

The WVHIN offers a Customer Care Team help desk to provide customers and end users with information and support related to WVHIN Services. Examples of issues that will be resolved directly by the third party include: WVHIN portal user support, password resets, new user setups, and panel upload problems. Depending on the nature of the issue, technical problems may be dealt with directly by a third-party vendor. The following types of issues will be escalated to a third-party vendor: system status, service problems, infrastructure problems, interface issues, connectivity problems, and other technical issues. For all reported problems, the Customer Care Team will work to find a resolution in a timely manner and update Participating Organizations of actions taken as appropriate. The Customer Care Team can be reached at:

1-844-468-5755
wvhinsupport@crisphealth.org

The WVHIN Customer Care Team is available 24 hours a day, 7 days a week. The WVHIN Customer Care Team is unavailable on the following holidays:

- New Year's Day
- Martin Luther King Jr. Day
- Memorial Day
- Juneteenth
- Independence Day
- Labor Day
- Thanksgiving Day
- Christmas Day

13. Audit

All Participating Organizations are required to monitor and audit access to and use of their information technology systems in connection with the WVHIN Services and in accordance with their usual practices based on accepted health care industry standards and applicable law. In the event the WVHIN chooses to exercise its right to audit a Participating Organization, the Participating Organization will provide the WVHIN with monitoring and access records upon request. The WVHIN regularly reviews the usage of Participating Organizations' and Authorized Users' access of Patient records, and will enforce any misuse by a Participating Organization and/or an Authorized User to include sanctions which may result in termination of access to the WVHIN's Services.

14. Breach Notification

14.1 Background and Purpose

A Breach occurs if Protected Health Information is acquired, accessed, used, or disclosed by an unauthorized person or entity in a manner not permitted under the HIPAA Privacy Rules. A Breach is presumed unless, through a documented risk assessment, a Covered Entity or Business Associate is able to demonstrate that there is a low probability that the Protected Health Information has been compromised. A risk assessment must consider at least the following factors:

(i) The nature and extent of the Protected Health Information involved, including the types of identifiers and the likelihood of reidentification;

(ii) The unauthorized person who used the Protected Health Information or to whom the disclosure was made;

(iii) Whether the Protected Health Information was actually acquired or viewed; and

(iv) The extent to which the risk to the Protected Health Information has been mitigated.

The notification process contemplated by federal and state law applies only if the Breach involves Unsecured Protected Health Information. Unsecured Protected Health Information means that the Protected Health Information has not been rendered unusable, unreadable, or indecipherable by unauthorized individuals or entities through the use of Encryption or other federally-approved technology. If a Breach occurs, but the Breach does not implicate any Unsecured Protected Health Information (the Protected Health Information is otherwise secured, i.e., through Encryption or destruction), then no notification is legally required.

Both federal and state laws require a notification to be made if there is a Breach of Unsecured Protected Health Information.

14.2 Obligations of Participating Organizations

Any Participating Organization which becomes aware of any known Breach involving Unsecured Protected Health Information disclosed through the WVHIN's Health Information Exchange must contact the WVHIN orally and in writing as soon as is reasonably practical, but in no event later than 24 hours after discovery. This notification shall include sufficient information to permit the WVHIN to begin its investigation process. A Participating Organization must cooperate with the WVHIN in the WVHIN's investigation of any known unauthorized disclosure of Protected Health Information.

Once a Participating Organization has received a written notice from the WVHIN that a Breach of Unsecured Protected Health Information has occurred, the Participating Organization shall determine whether it concurs with the written notification from the WVHIN. If the Participating Organization concurs that a Breach of Unsecured Protected Health Information has occurred, and any risk assessment is unable to demonstrate that there is a low probability that any affected Protected Health Information has been compromised, then the Participating Organization must notify each Patient affected by the Breach. This notification should be undertaken without unreasonable delay, but in no event later than 60 days after the date of its discovery.

The Participating Organization's notice to Patients must fully comply with the requirements of both the HITECH Act and its implementing regulations at 42 C.F.R. Part 164, Subpart D, as well as the West Virginia Code at Chapter 46A, Article 2A. The Participating Organization shall also undertake notice to prominent media outlets should the Breach involve more than 500 West Virginia residents, and notice to the Secretary of Health and Human Services, all in accordance with 42 C.F.R Part 164.

Notwithstanding any other provision of this Section 13, if a law enforcement official informs a Participating Organization that any notification or notice contemplated hereunder would impede a criminal investigation or cause damage to national security, then such notification or notice must be delayed for any and all periods of time authorized by the requirements of both the HITECH Act and its implementing regulations at 42 C.F.R. Part 164, Subpart D, as well as the West Virginia Code at Chapter 46A, Article 2A.

14.3 Obligations of the WVHIN

The WVHIN will maintain an internal incident reporting process designed to identify, internally report, investigate, and resolve known unauthorized disclosures involving Protected Health Information improperly disclosed through the WVHIN's Health Information Exchange. All unauthorized disclosures of Protected Health Information involving the WVHIN will be investigated immediately upon discovery. This report may be originated by a member of the WVHIN Workforce,

or by a member of the Workforce of a contractor or Business Associate Subcontractor to the WVHIN.

The WVHIN will report any known use or disclosure of information not provided for by its Business Associate Agreement to any affected Participating Organization. The WVHIN may also ask the affected Participating Organization to assist and otherwise participate in the investigation of the incident.

If a Breach has occurred, the WVHIN will notify any Participating Organization from which the Unsecured Protected Health Information originated. The WVHIN will also develop a plan to mitigate any harm to Participating Organizations and their Patients, to the extent that is practicable. This notice to the Participating Organization must comply with the requirement for Business Associates set forth in the HITECH Act and its implementing regulations at 42 C.F.R. Part 164, Subpart D. This notification must be undertaken without unreasonable delay and as soon as possible, but in no event later than five (5) business days after the Breach was initially discovered. The WVHIN will make its staff available to the Participating Organization as a consultative resource.

Each Participating Organization that receives written notification from the WVHIN of a Breach of Unsecured Protected Health Information will retain the ultimate authority to determine whether Protected Health Information has been compromised pursuant to the applicable requirements under the HITECH Act and its implementing regulations at 42 C.F.R. Part 164, Subpart D. In addition, each Participating Organization will retain the ultimate authority to determine whether a Breach under the West Virginia Code at Chapter 46A, Article 2A, is actionable. In making this determination, each Participating Organization may act in accordance with its own policies and procedures, provided that such policies and procedures comply fully with aforementioned federal and state laws and regulations. The WVHIN will also provide notice of the Breach to its Board of Directors without unreasonable delay and as soon as possible.

After any Breach, the WVHIN will undertake a root cause analysis of the circumstances surrounding the underlying Breach, and will determine what organizational or operational changes in its system, network privacy, network security, Workforce training, policies, and procedures are needed to protect against future Breaches.

15. Complaint Handling

Any person or organization who desires to file a complaint with the WVHIN about actual WVHIN operations or ancillary services may do so in writing, utilizing the Complaint Form published on the WVHIN website. All complaints will be directed to the WVHIN's Privacy Officer for handling. Complaints may be filed in person, by mail, or via email.

A complainant may request that the WVHIN maintain the confidentiality of the identity of the complainant. The WVHIN will respect this request for confidentiality unless, by doing so, it would place the complainant or any other person at significant risk or physical, mental, or financial harm, or unless disclosure is otherwise required by law.

The Privacy Officer will acknowledge the complaint to the complainant, initiate a review, and if necessary, investigate the facts and circumstances surrounding the complaint. Based upon this review and investigation, the Privacy Officer will determine if the complaint can be verified or not. If a complaint cannot be verified, then no further action by either the Privacy Officer or the WVHIN is required other than to notify the complainant that the complaint could not be verified.

If a complaint is verified, then the WVHIN will determine what actions are required to resolve the complaint. Such actions could include system changes, procedural changes, revised security efforts, harm mitigation, sanctions of the WVHIN staff or its Business Associates, or any other measure deemed necessary by the WVHIN to provide a fair, equitable, and effective resolution of

the complaint. The complainant will be notified of the resolution agreed upon by the WVHIN, if any, in writing.

All complaints shall be resolved by the WVHIN within six (6) months from the WVHIN's receipt of the complaint. The WVHIN shall notify the complainant of the WVHIN's resolution or other response to the complaint in writing.

A complainant may elect to file a complaint with the United States Department of Health and Human Services, Office of Civil Rights, if his/her/its rights under the law have been violated. The WVHIN will not retaliate against a complainant for filing a complaint.

16. Provider Authorization

Participating Organizations, by electing to receive data through WVHIN Services, authorize the WVHIN to transmit results, reports, and other Protected Health Information directly from Participating Organization's ancillary Health Care Providers, such as clinical laboratories and radiology centers. Participating Organizations further acknowledge the following:

(i) All ancillary Health Care Providers only represent that, at the time the data is transmitted by the ancillary Health Care Provider, the data transmitted is an accurate representation of the data that is contained in, or available through, the ancillary Health Care Provider's system;

(ii) Nothing in the Participation Agreement, Policies and Procedures, or otherwise will impose responsibility or liability on ancillary Health Care Providers related to the accuracy, content, or completeness of any data or information provided in connection with a message or otherwise;

(iii) As a data source, ancillary Health Care Providers do not assume any control over or responsibility for the clinical decision making as to any Patient of a Participating Organization; and

(iv) If not approved by ancillary Health Care Provider for delivery of report of record, access to such data through the WVHIN Services is neither designed nor intended to replace the ancillary Health Care Provider's principal method of results delivery to a Participating Organization and does not constitute a "Report of Record."

17. Standards

The WVHIN aims to support the WVHIN Services in a standards compliant manner and will use best practices and generally accepted standards, when possible and appropriate, that are recognized by state, federal, and/or industry authorities.

18. Policies and Procedures Amendments

These Policies and Procedures shall be available on the WVHIN's website at www.wvhin.org. The WVHIN may amend these Policies and Procedures from time to time at its discretion and shall post all revisions to its website. The Participant's Point of Contact shall be notified in writing of such changes. Any changes shall be effective 30 days following adoption by the WVHIN, unless the WVHIN determines that an earlier effective date is required to address a legal requirement, an imminent concern related to the privacy or security of Protected Health Information, or an emergency situation. The WVHIN may also postpone the effective date of a change if it determines, in its sole discretion, that additional implementation time is required.