



Washington State Health Information Exchange
OneHealthPort HIE Security Policy
Effective Date: 3/1/2011

This OneHealthPort HIE Security Policy is published by OneHealthPort and applies to the operation and use of the HIE Services by any Participant in the OneHealthPort HIE.

This Security Policy applies to all WA HIE Participants and HIE Users, and is subject to the applicable Participation Agreement and the OneHealthPort HIE Participation Terms and Conditions. The Participation Terms and Conditions are available at the HIE Reference site at <http://www.onehealthport.com/HIE/index.php>. Additional important information is provided in the OneHealthPort HIE FAQs and the OneHealthPort HIE Glossary, available at <http://www.onehealthport.com/HIE/index.php>.

The following obligations and requirements are intended to provide for the security of the HIE Services, transactions conducted using the HIE Services, and of the information maintained, stored or transmitted by, through or in the HIE Services.

1. SECURITY OF HIE SERVICES. OneHealthPort shall maintain, or if applicable obtain reasonable assurances that Services Vendors maintain, Reasonable and Appropriate Safeguards for the HIE Services and any Protected Information maintained or stored or in transmission through the HIE Services, or otherwise in the possession or control of OneHealthPort or any Services Vendor for purposes of the OneHealthPort HIE, as required by the Security Rule and consistent with the HIE Policies. OneHealthPort may implement supplemental or more stringent safeguards which OneHealthPort deems appropriate in OneHealthPort's reasonable discretion.

2. PARTICIPANT SECURITY ADMINISTRATION. The Participant shall maintain Reasonable and Appropriate Safeguards for its Workforce, Facilities, Information Systems and Authorized Devices used in connection with any Services, including but not limited to the following:

a. *HIE User Clearance.* Policies and procedures providing for reasonable and appropriate determination of the access privileges of HIE Users.

b. *HIE User Authorization.* Policies and procedures for authorizing, and suspending and terminating the authorization of its HIE Users who are authorized to access and use any of the HIE Services and obtain or disclose Protected Information through the HIE Services, on behalf of the Participant.

c. *HIE User Access Limitations.* Policies and procedures requiring HIE Users to limit their

access to and use of the HIE Services and Protected Information available through the HIE Services to the Minimum Necessary (except for Treatment purposes), and consistent with applicable federal and state law and the HIE Policies.

d. *Acceptable Use Management.* Acceptable use management services for the Participant's Information System(s) and Workstations by any HIE User of the Participant's Information System(s) or Workstations

e. *Access Controls.* Administrative, physical and technical access control Safeguards to prevent parties not authorized as HIE Users by the Participant from using the Participant's Information System(s) to seek or obtain access to any of the HIE Services, Protected Information available through the HIE Services, or any other Information System, and to detect and respond to any such unauthorized activity.

f. *Workstation and Device Management.* Policies and procedures for the authorization and secure operation and disposal of all Authorized Devices which the Participant permits its HIE Users to use in order to access any HIE Service. OneHealthPort may limit or prohibit the use of certain types of device as Authorized Devices, for example smartphones, if their security has not been adequately demonstrated to OneHealthPort's satisfaction in its sole discretion.

g. *Protected Information Lifecycle.* Policies and procedures governing the retention, inclusion in

OneHealthPort HIE
OneHealthPort HIE Security Policy

Effective Date: 3/1/2011

Page 2 of 4

records and disposal or destruction of Protected Information obtained by or through any Service.

h. *HIE User Training.* Appropriate and adequate training to all HIE Users in the requirements of applicable federal and state laws, the OneHealthPort HIE policies and procedures and all applicable Schedules.

i. *Sanctions for Violations.* Sanctions and disciplinary procedures for the Participant's HIE Users and other members of the Participant's Workforce and any other person subject to the Participant's authority, for accessing or using any HIE Service in violation of applicable federal or state laws, any HIE policy, procedure or Schedule, or the Participant's policies, procedures or technical controls implemented for purposes of access to and use of the HIE Services.

j. *Audit Trails.* Audit logs for transactions in which any Protected Information is transmitted to or from any of the HIE Services and the Participant's Information System(s) or Authorized Devices.

k. *Software Management.* Patch management, change management and updating policies and procedures for hardware and software included in the Participant's Information System(s) and Authorized Devices which may be used to access any HIE Service.

l. *Malware Protection.* Anti-virus and other anti-malware software or other applications intended to identify, prevent the download of, disable, uninstall or otherwise affect any computer virus, worm, "Trojan horse," spyware, or other potentially harmful software in or accessing Participant's Information System(s) or Authorized Devices, and/or using them to access any HIE Service, or the Information System of any party.

m. Any other Safeguard OneHealthPort has determined is Reasonable and Appropriate to protect (a) any Service, (b) the Information System or Authorized Devices of any party, or (c) any information, including but not limited to Protected Information, subject to review by the Community Oversight Organization.

3. SECURITY INCIDENTS AND BREACHES.
OneHealthPort, all Participants and all HIE Users

shall comply with the following Security Incident and Breach Response Policies:

3.1. Monitoring.

3.1.1. HIE Services Monitoring. OneHealthPort shall be responsible for monitoring or providing for the monitoring of all activity in the HIE Services, and in any Information System used to host, operate or manage a HIE Service, and at Facilities where equipment used to host, operate or manage the HIE Services is located.

3.1.2. Participant Monitoring. Each Participant shall be responsible for monitoring activity on its Information System(s), on its Workstations and other Authorized Devices, and at its Facilities.

3.2. Reporting of Security Incidents and Unauthorized PHI Uses/Disclosure.

3.2.1. OneHealthPort Reporting. OneHealthPort shall report to the Participant any Security Incident or Unauthorized Use or Disclosure of Protected Health Information of which it becomes aware which affects, or may affect, Protected Information of the Participant, as provided in the Operating Manual.

3.2.2. Participant Reporting. Each Participant shall report to OneHealthPort any Security Incident or Unauthorized Use or Disclosure of Protected Health Information of which it becomes aware, which may affect or involve the use or access to any HIE Service. Participants may report Security Incidents and Unauthorized Use or Disclosure of Protected Health Information to OneHealthPort at info@onehealthport.com.

3.2.3. HIE User Reporting. All HIE Users shall report to their Participant any Security Incident or Unauthorized Use or Disclosure of Protected Health Information which they become aware, may affect or involve the use or access to any HIE Service.

3.3. Security Incident Investigation.

3.3.1. OneHealthPort Investigation. OneHealthPort shall investigate any Security Incident which may affect or have affected any HIE Service or any Information System used to host, operate or manage a HIE Service, or any

OneHealthPort HIE
OneHealthPort HIE Security Policy

Effective Date: 3/1/2011

Page 3 of 4

Protected Information maintained, stored or in transmission or processing in a HIE Service, promptly upon receiving notice from a Participant or other information which reasonably indicates the potential occurrence of a such an event. OneHealthPort shall document the results of each such investigation. OneHealthPort shall provide for reasonable periodic reporting of Security Incident information to the Participant, and shall promptly report any Security Incident to Participant which presents or indicates a potentially material threat to the Participant's Protected Information, Information System(s) or Authorized Devices, or which may constitute a Security Breach.

3.3.2. Participant Investigation. Each Participant shall investigate any reported Security Incident involving access to or use of any HIE Service (a) from or by use of Participant's Information System or any other equipment or device of Participant, Authorized or otherwise, (b) by use of a user name and/or password issued to a HIE User of the Participant, or (c) by an HIE User of the Participant contrary to any OneHealthPort HIE policy or procedure, promptly upon receiving notice from OneHealthPort or other information which reasonably indicates the occurrence of such an event. The Participant shall document the results of each such investigation. The Participant shall permit OneHealthPort to review such documentation on a reasonable basis, and shall promptly report to OneHealthPort any Security Incident which presents or indicates a potentially material threat to any HIE Service or any other Participant's Protected Information, Information System(s) or Workstations or other equipment or devices, or which may constitute a Security Breach.

3.4. Security Incident Mitigation and Remediation. All affected parties shall share information about the results of their Security Incident investigations, and cooperate in determining and implementing measures to mitigate the harmful effects of any given incident and prevent other incidents of the same type, to the extent practicable.

3.4.1. Law Enforcement Notification. Any party may notify appropriate law enforcement agencies in the event it believes a Security Incident which affects it is a crime or the result of criminal activity.

3.4.2. Security Breach Notification. In the event a Security Incident or Unauthorized Use or Disclosure of Protected Health Information is also a Security Breach the parties shall notify potentially affected individuals and applicable regulatory authorities as follows:

a. Each affected Participant which has a direct provider-patient, plan-member or entity-customer relationship with potentially affected individuals shall have primary responsibility for their notification, if required by law or elected by the Participant.

b. Each affected Participant is primarily responsible for notification of regulatory authorities, if required by law or elected by the Participant.

c. Any notification to potentially affected individuals or to regulatory authorities shall be deemed notification as well by OneHealthPort (and any affected Services Vendor, if applicable) and each shall be identified as a notifying party, unless such party directs otherwise in writing.

d. In the event an affected Participant elects not to or fails to timely notify potentially affected individuals or regulatory authorities as provided above, and OneHealthPort reasonably determines that it may be required to give such notification by law, OneHealthPort may give such notification at its discretion.

4. ONEHEALTHPORT REMEDIES FOR PARTICIPANT SECURITY MANAGEMENT FAILURE. In the event that OneHealthPort determines that a failure by a Participant to comply with Section 2 of this Security Policy creates a material vulnerability potentially affecting (a) any HIE Service, (b) the Information System or any other equipment or device of any party, or (c) any information, including but not limited to Protected Information, OneHealthPort shall promptly notify the Participant and may, at OneHealthPort's reasonable discretion, suspend or limit access to and/or use of some or all of the HIE Services by some or all of the Participant's HIE Users, and/or from some or all of the Participant's Information System(s) and/or Authorized Devices, as OneHealthPort may determine is reasonably prudent. Such a failure by the Participant shall be deemed a Curable Breach, provided that upon receipt of notice of such a breach the Participant shall use its best efforts to come into compliance with this Security Policy. Upon the Participant's demonstration to OneHealthPort that the Participant is in compliance

OneHealthPort HIE
OneHealthPort HIE Security Policy

Effective Date: 3/1/2011

Page 4 of 4

with this Security Policy, OneHealthPort shall terminate the suspension unless other information available to OneHealthPort indicates that the material vulnerability continues. In the event of a continuing failure to come into compliance by the Participant, OneHealthPort may proceed to terminate the Participation Agreement as provided in the Participation Terms and Conditions.

5. PARTICIPANT REMEDIES FOR HIE SERVICES SECURITY MANAGEMENT FAILURE. In the event that the Participant determines that a failure by OneHealthPort to comply with Section 1 of this Security Policy creates a material vulnerability potentially affecting (a) the Participant's Information System or (b) any information, including but not limited to Protected Information, accessible in or through the Participant's Information System, the Participant shall promptly notify OneHealthPort and may, at the Participant's sole discretion, suspend or limit access to and/or use of any or all of the Services by some or all of the Participant's HIE Users, and/or from the Participant's Information System(s), as the Participant may determine is reasonably prudent in order to mitigate the vulnerability. Such a failure by OneHealthPort shall be deemed a Curable Breach, provided that upon receipt of such notice OneHealthPort shall use its best efforts to come into compliance with this Security Policy. Upon OneHealthPort's demonstration to the Participant that OneHealthPort is in compliance with this Security Policy the Participant shall terminate the suspension unless other information available to the Participant indicates that the material vulnerability continues. The Participant shall not be liable for any fees payable for any of the Services during any period of suspension under this Section, or for any reactivation fees following such suspension.