



LOUISIANA  
HEALTH CARE  
QUALITY FORUM

# LOUISIANA HEALTH INFORMATION EXCHANGE (LaHIE)

---

## STRATEGIC AND OPERATIONAL PLAN UPDATE

---

*Submitted to:*

The Office of the National Coordinator  
For Health Information Technology

U.S. Department of  
Health and Human Services

**June 2012**

8550 United Plaza Blvd., Ste. 500  
Baton Rouge, LA 70809  
[www.lhcqf.org](http://www.lhcqf.org)

## Table of Contents

<b>Introduction</b> .....	<b>3</b>
<b>1. Changes in HIE Strategy</b> .....	<b>4</b>
<b>2. Sustainability</b> .....	<b>32</b>
<b>2.1 Methodology</b> .....	<b>32</b>
<b>2.2 Sustainability Plan</b> .....	<b>34</b>
<b>2.3 Financial Objectives and Overview</b> .....	<b>35</b>
<b>2.4 Pricing Strategy</b> .....	<b>35</b>
<b>2.5 Key Adoption Rate Assumptions and Basis for Sustainability</b> .....	<b>36</b>
<b>2.6 Revenues</b> .....	<b>37</b>
<b>2.7 Conclusion</b> .....	<b>38</b>
<b>3. Evaluation Plan</b> .....	<b>39</b>
<b>3.1 Introduction</b> .....	<b>39</b>
<b>3.2 Assessment and Strategy</b> .....	<b>39</b>
<b>3.3 Louisiana HIE Evaluation Framework</b> .....	<b>40</b>
<b>3.4 Objectives for Obtaining Data</b> .....	<b>47</b>
<b>4. Privacy and Security Framework</b> .....	<b>49</b>
<b>4.1 Overview</b> .....	<b>49</b>
<b>4.2 Domain: Openness and Transparency</b> .....	<b>49</b>
4.2.1 Description of Approach and Corresponding Policies .....	49
4.2.2 Description of Stakeholder Outreach .....	51
4.2.3 Description of Gap Area .....	51
<b>4.3 Domain: Collection, Use and Disclosure Limitation</b> .....	<b>52</b>
4.3.1 Description of Approach and Corresponding Policies .....	52
4.3.2 Description of Stakeholder Outreach .....	53
4.3.3 Description of Gap Area .....	54
<b>4.4 Domain: Safeguards</b> .....	<b>54</b>
4.4.1 Description of Approach and Corresponding Policies .....	54
4.4.2 Description of Stakeholder Outreach .....	56
4.4.3 Description of Gap Area .....	56
<b>4.5 Domain: Accountability</b> .....	<b>56</b>
4.5.1 Description of Approach and Corresponding Policies .....	56
4.5.2 Description of Stakeholder Outreach .....	59
4.5.3 Description of Gap Area .....	59
<b>4.6 Domain: Individual Access and Correction</b> .....	<b>59</b>
4.6.1 Description of Approach and Corresponding Policies .....	59
4.6.2 Description of Stakeholder Outreach .....	61
4.6.3 Description of Gap Area .....	61
<b>4.7 Domain: Data Quality and Integrity</b> .....	<b>61</b>
4.7.1 Description of Approach and Corresponding Policies .....	61
4.7.2 Description of Stakeholder Outreach .....	62
4.7.3 Description of Gap Area .....	62
<b>4.8 Domain: Individual Choice</b> .....	<b>63</b>
4.8.1 Description of Approach and Corresponding Policies .....	63
4.8.2 Description of Stakeholder Outreach .....	64
4.8.3 Description of Gap Area .....	64

<b>5. Project Management Plan .....</b>	<b>65</b>
<b>5.1 Update on Major Activities - LaHIE Implementation Plan, Major Milestones with Timelines .....</b>	<b>65</b>
<b>5.2 Updated Staffing Plan .....</b>	<b>67</b>
<b>5.3 Updated Discussion of Risks and Mitigation Strategies.....</b>	<b>70</b>
5.3.1 External Risks.....	70
5.3.2 Internal Risks .....	71
<b>6. Tracking Program Progress.....</b>	<b>73</b>
<b>7. Appendices .....</b>	<b>76</b>
<b>7.1 LaHIE Participant Agreement.....</b>	<b>77</b>
<b>7.2 Email Authorization Dated December 2011 .....</b>	<b>78</b>
<b>7.3 Updated Organizational Chart .....</b>	<b>79</b>
<b>7.4 LaHIE Policy Manual .....</b>	<b>80</b>

## Introduction

Many entities in Louisiana have undertaken efforts to improve health care delivery with various quality and electronic health record initiatives. However, the existing electronic health records (EHRs), patient tracking, and care delivery systems are, at best, only partially connected across the multiple provider models throughout the state. There is limited interoperability between systems which results in difficulties in care coordination and information access, redundant costs, patient safety risks, lower quality, and operational inefficiencies. It also hinders the ability to obtain data for population health management and improvement.

Thus, Louisiana Health Care Quality Forum (referred to as “LHCQF”), a 501(c) (3) nonprofit entity, has undertaken to establish a statewide Louisiana Health Information Exchange (LaHIE). In March 2010, the Office of the National Coordinator for Health Information Technology awarded the LHCQF \$10.5 million to rapidly build capacity for exchanging health information across the health care system both within and across states.

In February 2011, LHCQF’s first Strategic and Operational Plan (SOP) was approved by the ONC. To date, LHCQF has implemented the plan, as outlined, with fidelity. Much progress was made since February 2011, including implementation and launch of LaHIE with active exchange of health information occurring and Direct messaging, and the establishment of agreements and policies and procedures as identified by the Legal and Policy workgroup and in compliance with HIPPA Privacy and Security rules and regulations, and the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health information.

This document consists of the first update to the original SOP, and is aligned with the requirements outlined in ONC-HIE-PIN-002, and ONC-HIE-PIN-003. It is organized as follows:

1.	<b>Changes in HIE Strategy</b> outlines major proposed changes to particular aspects of the original SOP. Where appropriate, the budget impact of the proposed changes are provided.
2.	<b>Sustainability Plan</b> provides an outline of the environment that LHCQF is creating for sustainability of health information exchange, as well as a business plan for the sustainability of any services directly offered or funded by the Grantee.
3.	<b>Program Evaluation</b> outlines LHCQF’s annual evaluation plan. This will supplement and provide information for the ONC’s national program evaluation.
4.	<b>Privacy and Security Framework</b> provides LHCQF’s framework to ensure a set of robust privacy and security policies and practices.
5.	<b>Project Management Plan</b> provides an update to the plan presented in the original SOP.
6.	<b>Tracking Program Progress</b> reports on progress on key measures identified by ONC, and sets annual targets for these key measures.
7.	<b>Appendices</b> <ul style="list-style-type: none"><li>- Participant Agreement</li><li>- Email Authorization dated December 2011</li><li>- Updated Organizational Chart</li><li>- LaHIE Policy Manual</li></ul>

## 1. Changes in HIE Strategy

Domain/Sections	Short Description of Approved Portion of SOP that Grantee is Proposing to Change (include page numbers)	Proposed Changes	Reason for the Proposed Changes	Budget Implications of Proposed Changes
<b>Overall HIE Strategy including Phasing</b>				
	<p><b>Page 65</b> - The original LaHIE timeline and strategy envisioned that Phase I and Phase II would occur concurrently. It was stated that Phase III development and implementation should begin in 4Q 2011 and would run in parallel to continued Phase II roll out and connections. It was anticipated that Phase III functions would begin to be available for organizations beginning in 1Q 2012.</p>	<p>The overall LaHIE strategy proposed in the original Strategic and Operational Plan will not fundamentally change. Phases I and II are in production and LaHIE will continue to demonstrate utilization prior to fully implementing Phase III. We would like approval to begin development and implementation of Phase III as noted in the approved Strategic and Operational Plan (SOP) in parallel with continued roll out of Phase II so that we can support the MU and Crescent City Beacon Collaborative (CCBC) initiatives in the state, i.e., HIE to HIE exchange (Spring/Summer 2012).</p>	<p>LaHIE would like to begin development and implementation of Phase III (as noted in the approved SOP) in parallel with continued roll out of Phase II so that we can support Meaningful Use and the Crescent City Beacon Community (CCBC) initiatives.</p>	<p>The project budget was approved with a phased approach; therefore, no further changes to the budget are required. Previously budgeted Phase III funds for development and implementation will need to be accessed.</p>

Domain/Sections	Short Description of Approved Portion of SOP that Grantee is Proposing to Change (include page numbers)	Proposed Changes	Reason for the Proposed Changes	Budget Implications of Proposed Changes
<b>Governance</b>				
<p><b><u>Removal of Committee; Change of Name</u></b></p>	<p><b>Page 35 (Collaborative Governance Model) and Page 39 (organizational chart), page 100, pages 39 - 42:</b> As noted in the approved SOP on page 35, the LHCQF is the governing body of LaHIE. The current LHCQF committee structure outlining five committees (noted on page 36 of the SOP) was changed by LHCQF's Board of Directors during its 2011 strategic planning session. The previous committees will serve as task forces when needed and appropriate, and will not be standing committees. However, the HIT Advisory Council will replace the HIE Steering Committee (new name).</p>	<p>LHCQF Board of Directors will be the primary governing body over LaHIE. The HIT Advisory Council (new name) is active and will continue to consist of an independent group of health IT experts and health care consumers that represent the Louisiana health care environment. The Council membership will consist of no more than fifteen (15) members, serving as a representative body for the following stakeholder groups:</p> <ul style="list-style-type: none"> <li>• Hospitals/Health Systems</li> <li>• Physicians</li> <li>• Consumers</li> <li>• Payers/Health Plans</li> <li>• Employers/Businesses</li> <li>• Other health care providers (i.e. Pharmacies, Clinical and Reference Labs, Nursing Homes, Home Health, etc.)</li> </ul>	<p>Governance remains inclusive, transparent and attuned to the needs of the public. LHCQF observed that there was no need to create an additional committee, which added a new layer of bureaucracy that would impede flexibility and slow the movement of the project. An updated organizational chart is included in Appendix 7.3.</p>	<p>Neutral.</p>

		<p>The State HIT Coordinator and the Director of Health IT for LHCQF will serve as co-chairs of the HIT Advisory Council. A member of the Board of Directors will serve as a Board Liaison to the HIT Advisory Council. The HIT Advisory Council shall meet monthly (i.e., face-to-face or by teleconference). Ad hoc task forces may be assigned to address specific needs (e.g., health care financing and reimbursement, legal/policy, etc.).</p> <p>The HIT Advisory Council is accountable to the full Board of Directors for establishing and meeting measurable goals and objectives and acceptance of these duties and responsibilities:</p> <ul style="list-style-type: none"><li>• To provide strategic direction and assist in the implementation of LaHIE.</li><li>• To contribute to the efficient operation of the HIT programs, including LaHIE and LHIT Resource Center.</li></ul>		
--	--	--	--	--

		<ul style="list-style-type: none"><li>• To make recommendations to the full Board of Directors and provide the information the group needs to make a sound decision, or to communicate effectively a decision made by the group.</li><li>• To generate innovative ideas on how health IT can meet the escalating demands within the health care environment.</li><li>• To be the body to whom the Board of Directors looks to drive HIT initiatives.</li><li>• To serve as subject matter/content experts to the staff and LHCQF as it relates to health IT.</li><li>• To provide guidance and advice with regard to federal (i.e., ONC) and state (i.e., DHH) HIT directives and initiatives.</li></ul>		
--	--	--	--	--

Domain/Sections	Short Description of Approved Portion of SOP that Grantee is Proposing to Change (include page numbers)	Proposed Changes	Reason for the Proposed Changes	Budget Implications of Proposed Changes
<u>Bylaws</u>	<p><b>Page 42- 52</b>– Since the writing of the original SOP, the LHCQF (the governing body for LaHIE) has undergone two revisions of the bylaws that govern the organization.</p>	<p>The original SOP included the Second Restated and Amended Bylaws. In November 2011, the organization’s board of directors adopted the Fourth Restated and Amended Bylaws. Substantial changes that might have an impact on the operations of LaHIE are summarized below:</p> <ul style="list-style-type: none"> <li>• Principal office has changed locations. Current address is 8550 United Plaza Blvd., Ste. 500, Baton Rouge, LA 70809.</li> <li>• The Board of Directors’ terms have changed from varying terms (1 to 3 years) to three years for all directors.</li> <li>• References to a Medical Home Committee, a Health Information Technology Committee and a Quality Measurement Committee have been removed.</li> </ul>	<p>LHCQF updates its bylaws periodically, when the board of directors determines that a revision is necessary.</p>	<p>Neutral.</p>

		<ul style="list-style-type: none"><li>• Board officers will now serve a one-year term, rather than a two-year term.</li><li>• These changes have already been approved and implemented by the Board of Directors, and do not significantly impact the governance of LaHIE.</li></ul>		
--	--	--	--	--

Domain/Sections	Short Description of Approved Portion of SOP that Grantee is Proposing to Change (include page numbers)	Proposed Changes	Reason for the Proposed Changes	Budget Implications of Proposed Changes
<b>Technology</b>				
<b><u>Shifts in Phasing</u></b>	<b>Page 63 – 65</b> - The original deployment plan for LaHIE was comprised of four phases that encompassed the gradual development of the functionality of the system.	The shifting of three activities to Phase I, with prior approval from ONC. <b>Phase I:</b> <ul style="list-style-type: none"> <li>• Single Sign On (SSO) between EHR and</li> <li>• Direct Secure Messaging</li> <li>• Additional functionality with DHH services, i.e., registries, Medicaid Eligibility verification</li> </ul>	The changes in phases are due to market conditions and requests from stakeholders. LaHIE received approval from Veronica Jackson, ONC, on December 5, 2011 (see Appendix 7.2).	The project budget was approved with a phased approach; therefore, no further changes to the budget are required.
<b><u>Selection of Technology Vendor</u></b>	<b>Page 63, 163</b> - LHCQF indicated that it would develop and release a Request for Information and Request for Proposal in order to select a vendor to carry out the LaHIE Technical Architecture Model.	Through the RFP process, Orion was selected as the vendor of choice in Summer 2011 to implement the Technical Architecture Model for LaHIE.	N/A	N/A

<b>Domain/Sections</b>	<b>Short Description of Approved Portion of SOP that Grantee is Proposing to Change (include page numbers)</b>	<b>Proposed Changes</b>	<b>Reason for the Proposed Changes</b>	<b>Budget Implications of Proposed Changes</b>
<b>Financial</b>				
<b><u>Number of Potential Data Suppliers; Impact on Financial Modeling</u></b>	<b>Page 91</b> – The original plan outlined potential Data Suppliers practicing in Louisiana.	The total number of acute care hospitals according to the Louisiana Department of Health and Hospitals is 138.	Based on the pricing model provided by the contracted HIE vendor, many physicians will be included under the agreement with an acute care facility.	The impact is neutralized with pricing increases; however, the overall cost of the HIE is being sustained to a greater extent by non-payers in the current fee model.
<b><u>Transaction Based Services and Per-Enrollee Fee</u></b>	<b>Page 91</b> – LAHIE’s original pricing strategy included a per-enrollee fee through Medicaid and commercial health plans, an annual subscription fee for both hospitals and physicians, and an ad hoc service available on a fee per transaction basis.	The annual subscription fee will remain; however, we propose adjustments of the per-enrollee fee to a pro-rated enrollee fee model and removal of the fee per transaction component.	Feedback from stakeholders indicated that they intend to pay for services that directly impacted their population. Feedback from providers indicated that transaction fee models do not incent adoption of HIE services, and in fact, can be a deterrent. In addition, a shift to a model based on Commercial Health Plans’ population, pro-rated to those utilizing the exchange services	Removal of the fee per transaction charge leads to a \$135,000 annual decrease in revenues. Adjustment of the payer and Medicaid per-enrollee fee to a pro-rated model has a varying degree of impact as participation increases. The \$135,000 adjustment is neutralized with pricing adjustments described in Section 2 (Sustainability Plan). Average costs are comparable to the

			becomes necessary.	original model; however, the costs in Year 4 are higher. The current model provides for more variability which will allow the HIE to remain profitable at a lower break-even point.
<b><u>Pricing</u></b>	<b>Page 91-92</b> – The original plan outlined the annual operating cost to operate the HIE, along with associated pricing necessary to sustain the HIE.	The Sustainability Plan (See Section 2) outlines the current pricing approach necessary to sustain the exchange.	Proposed changes to the original plan are a result of HIE vendor pricing negotiations and numerous stakeholders discussions and negotiations.	Implications of the pricing changes are neutral as a whole, but do change the percentage mix of revenue sources.
<b><u>Revenue Projections and Annual Cost Estimates</u></b>	<b>Page 92 – 93</b> – In Year 1 (Oct. 2010), total annual cost estimates were projected at \$6.5 million, with costs decreasing to \$4 million in Year 4 (Oct. 2013). Revenue projections at full implementation were assumed to be \$4,207,000.	Current annual cost estimates are \$4.7 million, and revenue projections are \$5 million.	HIE vendor negotiations and the resulting technology costs have been the primary driver of this change. Implementing a hosted model reduced the initial investment and allows for cost to be more variable with participation rates.	Average annual costs are comparable to the original model; however, the costs in year 4 are higher. The current model provides for more variability, which will allow the HIE to remain profitable at a lower break-even point.
<b><u>Staffing Changes</u></b>	<b>Page 93 – 94</b> - The original plan outlined 4.3	The staffing changes are summarized in Section 5	See Section 5.	See Section 5.

	FTEs for HIE project activities, as well as numerous vendors for various professional services (technical architecture, accounting, legal, subject matter experts, evaluation, and auditing).	(“Project Management Plan”) of this document.		
--	---	---	--	--

Domain/Sections	Short Description of Approved Portion of SOP that Grantee is Proposing to Change (include page numbers)	Proposed Changes	Reason for the Proposed Changes	Budget Implications of Proposed Changes
<b>Business Operations</b>				
<b><u>Project Goals</u></b>	<b>Page 68</b> - The main goal for business operations was originally planned to focus on meeting the necessary requirements for Meaningful Use. This has not changed.	<p>Throughout the course of business operations, a set of more specific goals, measurable objectives and performance measures were identified. The updated goals are summarized below</p> <p><b>Goal 1: Enable the effective and efficient use of health information in optimizing patient safety, quality and resource utilization by individuals and organizations within Louisiana.</b></p> <p>1.1 Provide economic and clinical value to health care providers</p> <ul style="list-style-type: none"> <li>• Improve data extraction and reporting</li> <li>• Improve quality of care and outcomes</li> <li>• Control costs of health care</li> <li>• Reduce medical errors</li> </ul>	Clear goals and objectives provide better guidelines for performance measurement, evaluation, and progress tracking.	Neutral.

		<p>and redundant services</p> <ul style="list-style-type: none"><li>• Improve patient safety</li></ul> <p>1.2 Provide economic and clinical value to payers</p> <ul style="list-style-type: none"><li>• Improve data extraction and reporting</li><li>• Improve quality of care and outcomes</li><li>• Control costs of health care</li><li>• Reduce medical errors and redundant services</li><li>• Improve patient safety</li></ul> <p>1.3 Provide value to patients/consumers</p> <ul style="list-style-type: none"><li>• Improve quality of care and outcomes</li><li>• Enhanced patient/physician communication</li><li>• Control costs of health care</li><li>• Reduce medical errors and redundant services</li><li>• Improve patient safety</li></ul> <p><b>Goal 2: Provide timely access to patient centered health information required for patient care and population health.</b></p>		
--	--	---	--	--

		<p>2.1 Improve coordination between health care providers, in state and across states.</p> <ul style="list-style-type: none"><li>• Increase adoption of LaHIE over time</li><li>• Provide evidence of data sharing across systems</li></ul> <p>2.2 Support improvements in population health.</p> <ul style="list-style-type: none"><li>• Improve tracking of patients across providers</li><li>• Improve data extraction and reporting</li><li>• Improve patient awareness of chronic diseases</li><li>• Reduce health disparities</li><li>• Increase disease surveillance</li></ul> <p>2.3 Support state Medicaid initiatives</p> <ul style="list-style-type: none"><li>• Improve data extraction and reporting</li><li>• Improve tracking of patients across providers</li><li>• Enable quality reporting for CCN</li><li>• Facilitate collection of data for state registries (e.g. birth outcomes)</li></ul>		
--	--	---	--	--

		<p><b>Goal 3: Maintain business processes to ensure the integrity of privacy and security safeguards, reliability of information within the system and exchange availability.</b></p> <ul style="list-style-type: none"><li>• Adhere to the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act requirements for the protection of Protected Health Information (PHI).</li><li>• Ensure the accuracy and reliability of information provided via the HIE.</li><li>• Build caregiver trust such that they rely on the HIE to support clinical decision making as a normal part of their daily workflow.</li><li>• Establish 99%+ system availability</li></ul> <p><b>Goal 4: Generate sustainability by operating and adapting the business model to meet the changing needs of the State of</b></p>		
--	--	---	--	--

		<b>Louisiana.</b> <ul style="list-style-type: none"><li>• Achieve net positive cash flow</li><li>• Deliver services at a price point the market can bear</li><li>• Maintain flexibility to deploy enhanced services</li></ul>		
--	--	---	--	--

Domain/Sections	Short Description of Approved Portion of SOP that Grantee is Proposing to Change (include page numbers)	Proposed Changes	Reason for the Proposed Changes	Budget Implications of Proposed Changes
<b>Legal/Policy</b>				
<p><b><u>Shift from Opt-Out to Opt-In</u></b></p>	<p><b>Page 56, 57 -</b> The original plan envisioned that LaHIE would utilize an opt-out patient consent process, such that inclusion of patient information in the state HIE would occur by default.</p> <p><b>Page 71 -</b> The original plan also envisioned an opt-out policy for the ED Use Case, in which data sharing is assumed and automated unless the patient takes the required steps to opt-out upon presenting to the ED.</p>	<p>After thorough review of the Louisiana legislation by our Legal and Policy workgroup and further legal review, it was identified that Louisiana is considered an “opt-in” state. This means that a patient’s consent is explicitly required for his/her information to be accessed via LaHIE. If the consent has not been obtained and the patient presents in an emergency situation, his/her information may be accessed in LaHIE for emergency treatment purposes only. If a patient explicitly opts out of LaHIE, his/her information cannot be accessed, regardless of any emergency situation. After connecting to LaHIE, providers/hospitals are required by LaHIE policy to include language in their respective privacy policies that references the exchange of health</p>	<p>LHCQF originally anticipated introducing legislation to address the “opt-out” provisions in state law; however, stakeholders decided that due to other major legislative initiatives being promoted in the state, it was not the most appropriate time to pursue the “opt-out” legislation at this time. LaHIE continues to work with the provider associations, i.e., Louisiana Hospital Association, and the Louisiana State Medical Society, to pursue the changes needed. We continue to research other states’ progress on these initiatives. In addition,</p>	<p>Neutral.</p>

		information through LaHIE. These requirements are covered in LaHIE Policy <b><i>“Individual Choice for Sharing Information in LaHIE.”</i></b>	the “opt in” process allows individuals a reasonable opportunity and capability to make informed decisions about the use and disclosure of their individually identifiable health information as it relates to LaHIE.	
<b><u>Legal Liability</u></b>	<b>Page 57</b> – The original plan envisioned that State-level legislation would be required to include privacy breaches by health care providers within the definition of malpractice, and to define a health information exchange as a healthcare provider.	At this time, state-level legislation is not being pursued; however, we will continue to work with our provider associations and providers to provide support on this when needed.	Stakeholders decided that due to other major legislative initiatives being promoted in the state, it was not the most appropriate time to pursue this legislation. LaHIE continues to work with the provider associations, i.e. Louisiana Hospital Association and the Louisiana State Medical Society, to pursue the changes needed. In addition, we continue to research other states’ progress on these initiatives	Neutral.

Domain/Sections	Short Description of Approved Portion of SOP that Grantee is Proposing to Change (include page numbers)	Proposed Changes	Reason for the Proposed Changes	Budget Implications of Proposed Changes
<b>Strategies for e- Prescribing</b>				
<b><u>Usage of EMPOWERx e-prescribing Tool</u></b>	<b>Page 18</b> - The original plan envisioned potentially utilizing the EMPOWERx e-prescribing tool, which provides a select group of Medicaid providers a way to access patient prescription histories, interaction checking, and the secure transmission of prescriptions directly to the pharmacy.	The EMPOWERx e-prescribing tool was not used. In keeping with the ONC HIE program information notice (ONC-HIE-PIN-001), and with the original plan, LaHIE will not replace EMR e-prescribing and e-lab functionality, but will identify the gaps in these areas and provide the needed services to fill those gaps. We propose to continue to identify needs and work with EHR vendors and/or Orion (the HIE Vendor) to implement solutions.	The EMPOWERx project was de-funded in Louisiana 2010. The LaHIE project leadership initially hoped that the tool would still be operational and could be used to fill the white space, but this has not been the case.	Neutral.
<b><u>Shift to Focus on Outreach and Communications for Adoption</u></b>	<b>Page 18</b> - The original plan proposed an e-prescribing platform to help providers attain Meaningful Use.	We propose to develop a comprehensive communication and outreach plan to determine which pharmacies currently have these capabilities, and which do not. Then, we must determine the barriers to adoption and develop strategies to overcome them. This plan will include, but not be limited to, the following elements:	A recent (2011) study funded by the U.S. Department of Health and Human Services' (HHS) Agency for Healthcare Research and Quality (AHRQ), and published in the <i>Journal of the American Medical Informatics</i>	Funding will be necessary to conduct the outreach and the market research study/survey. These funds were budgeted in the overall HIE budget but will need to be spent during the upcoming year.

		<ul style="list-style-type: none"> <li>• Work directly with the Louisiana Independent Pharmacy Association, chain pharmacies, and providers to contact pharmacies directly and identify specific dates the pharmacies will begin eRx.</li> <li>• Identify the providers prescribing to the pharmacies that are on the SureScripts network, but are not receiving eRx. Those who are on the network but not receiving eRx will receive focused outreach.</li> <li>• Louisiana Department of Health and Hospitals (Medicaid office) is working with Louisiana Board of Pharmacy and the pharmacy school at the University of Louisiana - Monroe to develop strategies for increased outreach and education.</li> <li>• LHCQF participated in State legislative sponsored eRx workgroup and proposed</li> </ul>	<p><i>Association,</i> determined that physician practices and pharmacies generally view electronic prescribing as an important tool to improve patient safety and save time, but both groups face barriers to realizing the technology's full benefit. While physicians can qualify for Medicare and Medicaid electronic health record incentive payments by generating and transmitting more than 40 percent of all prescriptions to pharmacies electronically, as part of the HITECH Act of 2009, adoption is still problematic due to the barriers uncovered in the study. For example, prescription renewals, connectivity between physician offices and mail-order pharmacies, and manual entry of</p>	
--	--	--	--	--

		<p>a joint committee resolution in the 2012 legislative session.</p> <ul style="list-style-type: none"><li>• LaHIE will continue to evaluate providers ability to have access to e-prescribing technology, and may add this capability should it be required in the future.</li></ul>	<p>certain prescription information by pharmacists—particularly drug name, dosage form, quantity, and patient instructions—pose problems to pharmacies and practitioners alike.</p>	
--	--	---	---	--

Domain/Sections	Short Description of Approved Portion of SOP that Grantee is Proposing to Change (include page numbers)	Proposed Changes	Reason for the Proposed Changes	Budget Implications of Proposed Changes
<b>Strategies for Structured Lab Results Exchange</b>				
<p><b><u>Submitting Lab Results Electronically to OPH</u></b></p>	<p>The original plan envisioned LaHIE working directly with labs already submitting results electronically to OPH to capture results in LaHIE. Specific strategies were not outlined in the plan.</p>	<p>LaHIE is expanding beyond the original scope of facilitating eLR reporting to support Meaningful Use to advocate that lab results be sent electronically in all care settings. Our strategies include:</p> <ul style="list-style-type: none"> <li>• Developing relationships with reference-labs that are currently electronically submitting to OPH and arranging to have a copy of these results sent to LaHIE. This is a major initiative of the Secretary of Louisiana’s Department of Health and Hospitals, with a delivery timeline by June 30, 2012.</li> <li>• Actively pursuing arrangements with hospital labs and independent labs for lab results information to be displayed in LaHIE and exchanged via Direct.</li> </ul>	<p>Based on stakeholder input, the role of the HIE in lab exchange has evolved beyond assisting with meeting public health reporting requirements required for Meaningful Use. Effectively implementing these strategies will have a positive impact on the delivery of care to patients in Louisiana.</p>	<p>Funding for interfaces will be needed, but has been budgeted in the initial overall costs of the HIE system.</p>

		<ul style="list-style-type: none"> <li>The HIE and REC teams will work with EHR vendor community to adopt the LRI Guide when it is finalized. The LRI Pilot (Standards and Operability Framework Lab Results Interface is working to develop an “LRI Guide,” currently in draft phase, which focuses on identifying the requirements, specifications and standards, and on providing the implementation guidance for electronic reporting of ambulatory care laboratory test results in United States. (See Section below on “LRI Pilot.)</li> </ul>		
<p><b><u>Education and Outreach Efforts</u></b></p>	<p>A focused outreach and communication plan for adoption of structured lab results exchange capability was not identified in the original plan.</p>	<p>We propose to work with the hospitals and physicians participating in LaHIE and the REC to determine the labs to which they refer, and target outreach and onboarding efforts accordingly. Stakeholders were convened for strategic and operational planning updates in</p>	<p>As the LaHIE system matures and stakeholder input is received, we anticipate that we will continue to make adjustments like this throughout the project.</p>	<p>Funding will be necessary to conduct the outreach and the market research study/survey. These funds were budgeted in the overall HIE budget but will need to be spent during the</p>

		late February. A primary focus of this group was to solidify a viable and successful strategy and plan for lab exchange. This group will be reconvened if deemed necessary.		upcoming year.
<b><u>Participation in Standards and Operability Framework Lab Results Interface (LRI Pilot)</u></b>	Participation in the Standards and Operability Framework Lab Results Interface (LRI Pilot) was not included in the original plan.	We plan to research and monitor the efforts of the Standards and Operability Framework Lab Results Interface (LRI Pilot). The goal of the LRI pilot is to address the challenge of lab reporting to ambulatory primary care providers. The LRI Pilot is also working to develop an “LRI Guide,” currently in draft phase, which focuses on identifying the requirements, specifications and standards, and on providing the implementation guidance for electronic reporting of ambulatory care laboratory test results in United States.	There are at least two standard specifications for ambulatory laboratory reporting, neither of which are adopted universally across industry. The cost and time to initiate new electronic laboratory results interfaces hampers broad adoption of such interfaces. The field-by-field details of HL7 v2 implementation guides used by clinical labs and EHRs vary, creating a need for mapping or configuration per interface, and the prevalence of core subsets of LOINC codes for common tests and analytes also varies, causing	Neutral.

			<p>downstream issues in decision support and quality reporting. Participating in the LRI Pilot would allow LHCQF to access the knowledge and standards developed by stakeholders and participants from across the health care IT industry. When the LRI Guide is implemented, we plan to reach out to vendors to adopt the standards in the guide.</p>	
--	--	--	--	--

Domain/Sections	Short Description of Approved Portion of SOP that Grantee is Proposing to Change (include page numbers)	Proposed Changes	Reason for the Proposed Changes	Budget Implications of Proposed Changes
<b>Strategies for Care Summary Exchange</b>				
	<p><b>Page 28</b> - The original plan states that the secure messaging and provider directory features (to be built during Phase I of the Technical Infrastructure detailed in section IV.D.3) will allow for this early exchange of the care summaries. However, explicit strategies for advancing the Care Summary Exchange were not included in the original plan.</p>	<ul style="list-style-type: none"> <li>• Generate care summaries from the central repository and send them to the requesting EHR.</li> <li>• Query care summaries from IDN HIEs and send them to the requesting EHR.</li> <li>• Enable Direct messaging to connect providers, including the Crescent City Beacon Community providers. Work with REC to identify additional primary care providers for Direct Exchange. We will also identify the labs with which these providers do business to enable lab result delivery via Direct.</li> </ul>	<p>In the original plan, no specific strategies were developed for care summary exchange.</p>	<p>Neutral.</p>

Domain/Sections	Short Description of Approved Portion of SOP that Grantee is Proposing to Change (include page numbers)	Proposed Changes	Reason for the Proposed Changes	Budget Implications of Proposed Changes
<b>Sustainability</b>				
	<p><b>Page 88 – 91</b> - The original plan envisioned a sustainability strategy that was based on several core assumptions, which we believe are still true. However, many of the assumptions about have changed as a result of additional research, a more sophisticated understanding of the market and competition, and stakeholder feedback.</p>	<p>See Section 2 – Sustainability Plan.</p>	<p>See Section 2 – Sustainability Plan.</p>	<p>See Section 2 – Sustainability Plan.</p>

Domain/Sections	Short Description of Approved Portion of SOP that Grantee is Proposing to Change (include page numbers)	Proposed Changes	Reason for the Proposed Changes	Budget Implications of Proposed Changes
<b>Privacy and Security Framework</b>				
	<p><b>Page 88 – 91</b> - The original plan did not include a privacy and security framework, although the Communication plan (pages 98 – 114) did include general strategies to ensure that providers and patients are aware of the measures that LaHIE is taking to ensure that privacy and security concerns are addressed.</p>	<p>Please see “Privacy and Security Framework” in Section 4 of this document, which addresses the requirements in ONC-HIE-PIN-003, released on March 22, 2012.</p>	<p>See Section 4 – Privacy and Security Framework.</p>	<p>Budgetary implications include purchasing cyber-liability insurance as well as increase of D&amp;O coverage for the organization. In addition, authentication access could have budget implications and will need to be funded. Depending on the proposed costs after thorough review, these costs may need ONC approval.</p>

Domain/Sections	Short Description of Approved Portion of SOP that Grantee is Proposing to Change (include page numbers)	Proposed Changes	Reason for the Proposed Changes	Budget Implications of Proposed Changes
<b>Evaluation Plan</b>				
	<p><b>Page 26 – 30 - The</b> original SOP outlined a general assessment and evaluation strategy that leveraged and coordinated many groups that have complete or partial assessment metrics. Additionally, the general strategy envisioned annual reassessment and updates to the provider, hospital, pharmacy, lab, health plan, and public health surveys as well as metrics from HIE implementation and adoption and overall EHR adoption from the REC. Metrics were developed for Governance, Finance, Technical Infrastructure, Business &amp; Technical Operations, Legal/Policy, and Performance Measures.</p>	<p>LHCQF has issued an RFP for evaluation services in 2012. Prior to this time, we have consistently monitored and reported monthly to LHCQF Board of Directors, as well as Louisiana’s Department of Health and Hospitals and ONC on the overall assessment and status of LaHIE. The beginning metrics based on transactional data have been established.</p>	<p>The ONC has required the development of an evaluation plan in the PIN dated February 8, 2012.</p>	<p>The costs for the evaluation were included in budget; thus, the budget impact is neutral.</p>

## 2. Sustainability

### 2.1 Methodology

For the health information exchanges (HIEs) in varying stages of development, no business model has yet proven to offer a clear path to sustainability. Although financial start-up assistance from foundations and public-sector sources is increasing, alignment of incentives, return on investment and regulatory issues have to be addressed if HIEs are to maintain financial viability once they are operational.

A successful HIE is one that can sustain itself financially for the long term and is not reliant on long term public grant support. Thus, LaHIE has developed a plan to attract different sources of revenue. LaHIE developed financial models that produced a number of sustainability scenarios. These scenarios were comprised of complex variables that were manipulated based on assumptions made by LaHIE about the environment, demand, technological advances, etc. As stakeholder meetings occurred, model variables were updated to incorporate the information gathered in these discussions. From these scenarios, LaHIE selected a “conservative projection” scenario that is considered to be the “most likely” scenario based on the current HIE landscape. Given the nature of HIEs and the experience of other states, we anticipate that this model will continue to evolve over time for achieved results and adoption rates. This projection includes the following assumptions:

- Program must be sustained after federal funding runs out.
- Minimal volume assumptions including acute care hospitals only.
- Minimal payer contributions, calculated at a prorated hospital market share usage rate.

A combination of federal, state and private sector funding has been used to establish:

- An effective public-private Health Information Exchange (HIE) operating entity, with a representative governance model.
- The technology infrastructure to enable health information exchange and data collection for population health management.
- A sustainable business model that is value based and equitable to health care stakeholders.

The objectives for the LaHIE are to achieve a sustainable value-driven HIE that exchanges secure health information, to facilitate patient-centered meaningful use among stakeholders and support the management of population health. LaHIE strategically engages active stakeholder collaboration and takes a regional team approach to successfully plan and implement a unified LaHIE.

The initial use cases addressed in LaHIE’s Business and Sustainability Plan are:

- Care Coordination through the Clinical portal – clinical summary view
- Capability for Continuity of Care Document (CCD) exchange and publishing

- Submission of information to Public health entities – immunizations, electronic lab reporting and syndromic surveillance
- Common methodology for referral management, secure messaging and notifications
- Exchange of patient information

The initial implementation is supported by the following HIE foundation (core) services:

- Patient Identity Management
- Record Locator Service (RLS)
- Provider Registry
- User Identity Management and Authentication
- Secure Access and Audit Reporting
- Consent Management and Tracking

The guiding principles for this plan include:

- **Self-Sustainability with Revenues Aligned with Cost and Value.** LaHIE will be part of a financially self-sustaining not-for-profit organization that provides services that generate revenue aligned with the value to participants.
- **Requirement for Funding Prior to Breakeven.** LaHIE requires initial start-up funding to support infrastructure development, marketing, sales, and operations prior to self-sustainability. LaHIE plans to run cash flow positive in the first year of operations.
- **Creative/Alternative Revenue Sources.** LaHIE will continue to consider alternative revenue sources derived from other parties and services to defray costs of the LaHIE, but have not included any of these sources in the conservative financial model.
- **Shared Costs Model.** Those who use and benefit from LaHIE will share the costs of the system. This includes, but may not be limited to, hospitals, providers, payers, labs, pharmacies, hospice, home health and nursing homes.
- **Pricing Based on Value, Utilization, and Adoption.** LaHIE prices its services to promote rapid adoption and to encourage utilization so as to quickly move to a point of critical mass. Hospitals and payers will initially share in paying for the HIE because they will most likely receive the most value from the more readily accessible health information at the point of care. Furthermore, use of the HIE and EHRs positions them well for achieving future Meaningful Use requirements. Once hospitals and providers begin to properly use the system, the payers will benefit. Eventually, labs, pharmacies, hospice, home health, nursing homes, and others will share in the costs of the system.

In collaboration with the Louisiana Department of Health and Hospitals and Louisiana Medicaid, LaHIE is a critical component of Louisiana's Vision for Health Information Technology (HIT). HIT makes it possible for health care providers to better manage patient care through secure use and sharing of health information. Through the employment of HIT and LaHIE in Louisiana, LaHIE seeks to enable improvements in health, minimize variations in care and address disparities in health care delivery, positively impacting the quality, safety and efficiency of health care. Creating a network of health information sharing, providers should gain efficiency through productivity and a reduction in the burdens of documentation of duplicative procedures and/or tests. This will yield improved quality of care by enabling better clinical decision support

at the point of care and giving providers the ability to access the right information for the right patient at the right time.

In collaboration with DHH, LaHIE is targeting the following initiatives during 2012:

- Submission of immunizations through LaHIE via integration of the Louisiana Immunization for Kids Statewide (LINKS) program
- Submission via LaHIE of syndromic surveillance, infectious diseases, eLab reporting to DHH's Office of Public Health (OPH)
- Eligibility verification capability for Medicaid patients via LaHIE

LaHIE continues to work with Louisiana's DHH and other statewide stakeholders to develop services based on demand and offering value while filling market gaps. Some of these include:

- Working with the Louisiana Medicaid program in the rollout and deployment of their new Coordinated Care Network (CCN) programs, Bayou Health, leveraging LaHIE as an instrument for submission of quality reporting, increasing the demand for exchange between providers, as well as advancing patient centered medical/health homes and pay for performance initiatives.
- Working with all Health Plans in Louisiana, including Louisiana Medicaid, to create value for an all payers claims database in conjunction with patient clinical information.
- Working with the potential CMS "Partnership for Patients" grant funding opportunity in Louisiana as a method of streamlining communications through HIT among hospital staff, nursing facility staff, nursing facility residents' primary care providers and other specialists, pharmacies, and families. This grant proposal will be submitted in June 2012 and will focus on the "Initiative to Reduce Avoidable Hospitalizations among Nursing Facility Residents".
- Engaging community focused initiatives to increase provider engagement and adoption focusing on the "patient".

## 2.2 Sustainability Plan

In implementing LaHIE, it was necessary to identify all sources of revenue from startup to sustainability. Our goal of identifying revenue sources is informed by a number of factors, including:

- Any investment of state monies will be leveraged to achieve a sustainable business model. Ongoing state match funding was not an assumed revenue source for continued operations.
- Participants in the exchange will be willing to pay fees relative to the value that their particular institutions are gaining from the exchange. It was not assumed that participants will pay fees for value associated with the "greater good" or "community benefit" or "improved health."
- While potentially available for future projects and expansions, ongoing grant funding is not certain enough to include in a financial model.

- Revenue should not be sought disproportionately from any one stakeholder or group of stakeholders.
- Transaction fee models do not incent adoption of HIE services, and, in fact, can be a deterrent.
- Subscription fee models incent higher utilization of HIE services and, if properly developed, can provide stability in revenue planning.
- Financial incentives for EHR adoption, which have been legislated at the federal level, will improve the economic case for physicians and facilities to participate in the HIE, especially if “meaningful use” rules define HIE connectivity as being important.

To arrive at reasonable revenue estimates that met all of these criteria, LaHIE selected a model that began with a \$12 million investment of federal and state funds, and then relied upon projected participant subscription fees to achieve financial sustainability. The implication of this approach is that the initial investment must be used to build not only the core infrastructure, but will also fund the development of enough early services or use cases to justify the expense of fees from participants. LaHIE will also seek funding from philanthropic sources.

### **2.3 Financial Objectives and Overview**

A critical goal of LaHIE is to reach financial sustainability based on intrinsic value delivered to HIE stakeholders, including providers, payers, consumers, and others. A pro forma financial model indicates that LaHIE can operate on a self-sustaining basis after ONC grant funding is depleted in late 2013. Annual HIE operating costs are estimated at approximately \$ 4.4 million in the first year, increasing to approximately \$4.7 million in the fifth year of operation, with the HIE running cash flow positive in the first full year of operation. The first full year surplus is based in part on the utilization of the ONC grant funding.

### **2.4 Pricing Strategy**

LaHIE’s pricing strategy is based on an annual, tiered subscription fee for health care providers and a per-enrollee fee for Medicaid and commercial health plans. The basic assumptions are:

- Commercial payers, hospitals, the Medicaid program, other health care providers and physicians will be willing to pay for HIE services relative to value received.
- The pricing structure is a tiered approach for hospitals based on their net patient revenues and the services provided.
- The pricing structure for physicians and other health care providers, i.e. nursing homes, home health agencies, pharmacies, and labs will be a set annual subscription fee based on provider numbers.
- Hospital subscription fees will cover the costs of all of their employed and affiliated physicians and their support staff.
- Early Adopters Incentives are available for a limited time period.

- A commercial health plan and Louisiana Medicaid will contribute a pro-rated portion based on provider participation.

## 2.5 Key Adoption Rate Assumptions and Basis for Sustainability

Provider adoption and payer support are the two key variables that drive these financial projections. Given the existing affiliation of hospitals with physicians and other care delivery organizations, e.g. long term care and home care, and the accelerating trend toward health system ownership of physicians, we utilized the hospital adoption count as a proxy for overall health care organization adoption for the HIE. The pro forma assumes 61 hospitals, or 44% of the total of 138 acute care hospitals in the state, using the HIE by the fifth year of operation. LaHIE believes this is a very attainable level. This also implies that roughly 25% of Louisiana residents will have HIE availability and support for their care. These estimates are preliminary and subject to change. Adjustments are anticipated to the business model as adoption increases, benefits are measured, and long-term models are developed with the payer and state government communities.

The adoption rate for providers is dependent on what benefits they can achieve from participation. An Impact Assessment modeling tool has been developed for hospitals and health systems that allows them to estimate the financial benefits of HIE participation. Expected benefits accrue from several areas including:

- Reduced indigent care delivery cost
- Reduced cost from Medicare cases with 30 day readmissions
- Achievement of HITECH incentive payments and avoidance of penalties by meeting meaningful use of electronic health records
- Reduced systems interface cost savings
- Reduced costs for clinical information sharing

Depending on each organization's specific operating and information technology environment, and based on studies in other HIE markets<sup>1</sup>, the above benefits have the potential to provide a return to hospitals and health systems of their HIE investment. The economic benefit model is being tested and refined in conjunction with stakeholders as LaHIE matures, especially with early adopter organizations.

In order to attract payer support, payers will need assurance that the HIE has enough critical mass to make a positive impact on care delivery efficiencies, thus reducing cost of care delivery. This is a critical element of sustainability, as the HIE will not be sustainable solely on the basis of provider organization funding. In order to achieve this, it will be necessary to measure the benefits of the HIE working closely with the payer and provider participating organizations. As part of the implementation plan, LaHIE has begun developing a measurement approach to capture and report results that will be used as the basis for proving the economic benefits of the HIE to the payers. LaHIE is working with the payer community, including Department of Health and Hospitals (DHH), Blue Cross Blue Shield of Louisiana (BCBS LA), and other private sector

---

<sup>1</sup> Multiple sources: HIE studies conducted by eHealth Initiative, ONC information, and HIE Consultants

payers to continuously refine an on-going financial support model. LaHIE's industry research<sup>2</sup> is based on numerous sources that indicate, conservatively, potential savings of at least \$25 per member per year. This accrues to state Medicaid, self-insured employers and at risk private payer organizations.

LaHIE has secured letters of intent from BCBS LA and DHH to financially support the HIE, dependent on achieving PMPY savings. BCBS LA has approximately 1.1 million covered lives and Medicaid has approximately 1.2 million. Together, this represents a total of 2.3 million covered lives, a substantial percentage of the population in the state. LaHIE utilized the provider penetration percentage to develop a model that prorates the amount of per member per year (PMPY) funding support from the payers. This resulted in \$650 thousand in payer revenue in 2012 increasing to \$1 million in revenue in the fifth year of operation. This is a critical element of HIE sustainability.

## 2.6 Revenues

Federal and state subsidies allow for the development of core HIE service offerings from 2011 to 2013. These subsidies also provide an opportunity for LAHIE to heavily incent early adopters in 2012. This incentive of approximately \$2.6 million leads to an adoption rate of 29% by the end of 2012 and 44% by 2016. Payer sponsored subsidies are assumed to begin in 2012 at a rate of \$1.00 PMPY prorated to their market share.

2014 through 2016 show a stable and steadily growing revenue base once federal and state subsidies are discounted. Growth is driven solely by participation increases in market share, which is modeled at 13% compounded annual growth rate. Additional subscription fees for the various service enhancements are absorbed by LaHIE and not passed on to subscribers in this model. Additional revenue sources, including subscription fees for nursing homes, pharmacies, home health agencies, labs, first responders/ambulance services, etc., are not currently included in the financial model although there is active interest and participation within these health care providers.

Current hospital adoption projections are noted in Figure 1, below.

---

<sup>2</sup> Multiple sources: HIE studies conducted by eHealth Initiative, ONC information, HIE Consultants, and Wisconsin/Human study.

<b>LaHIE</b>						
<b>Revenue Model Assumptions</b>						
	2011	2012	2013	2014	2015	2016
Hospitals < \$10 Million	1	2	5	6	7	9
Hospitals >10M < \$25 Million	1	4	5	8	10	12
Hospitals >25M < \$100 Million	0	15	15	16	16	18
Hospitals >100M < \$175 Million	1	6	6	7	8	8
Hospitals >175M < \$225 Million	1	3	5	6	7	7
Hospitals >225M < \$300 Million	0	2	3	3	3	3
Hospitals > \$300 Million	0	3	3	3	3	4
<b>Total Hospital Participants</b>	<b>4</b>	<b>35</b>	<b>42</b>	<b>49</b>	<b>54</b>	<b>61</b>
Healthplan Covered Lives (Prorated)	0	649,508	779,410	909,311	1,002,098	1,132,000
Unaffiliated Physicians	0	25	50	75	100	125

**Figure 1: LaHIE Revenue Model Assumptions**

## 2.7 Conclusion

The Business and Sustainability Plan is a living document. Given the immaturity of the HIE industry, and the early phases of LaHIE, flexibility is critical to success. LaHIE must continue to be nimble and responsive to stakeholder needs, while maintaining a sharp focus on its mission. LaHIE has the potential to contribute in a major way to the transformation of health care delivery in the state of Louisiana, through enabling improvements in patient coordination of care, reducing unnecessary and redundant costs, improving safety and quality, increasing convenience for patients, and enabling population health management and wellness.

## **3. Evaluation Plan**

### **3.1 Introduction**

The goal of the following evaluation plan is to measure the performance and success of the Louisiana Health Information Exchange (LaHIE), and to support the overall goal set by the Office of the National Coordinator for Health Information Technology (ONC) to provide documentation of lessons learned, technical assistance, and program guidance based on the results. In order to attain our goal and to support the overarching goal of the ONC, LHCQF will contract with a third party to perform on-going LaHIE evaluation services. A Request for Proposal (RFP) has been developed and disseminated to national program evaluation vendors, as well as to universities within the state of Louisiana. Responses to the RFP are due by June 11, 2012, and vendor selection will take place by September 3, 2012.

Ultimately, LHCQF intends to use the qualitative and quantitative data collected to 1) identify pertinent and achievable metrics; 2) gain an understanding of the barriers and views of stakeholders; and 3) have the tools available to conduct future self-evaluations.

### **3.2 Assessment and Strategy**

LHCQF will contract with a third party to evaluate the Health Information Exchange (LaHIE) using a before and after study design, with the before being the initial submission of the Strategic and Operational Plan (SOP) in 2010, and after being the updates to the SOP in June 2013 and March 2014. These evaluations will provide information on the progress that LaHIE is making toward promoting the Health Information Exchange, the management of grant funds, the appropriate levels of stakeholder participation, and the overall impact that LaHIE is having on the health of Louisiana's residents. The evaluation will also provide information to ONC about the relative success of different approaches to implementing HIE, and the success of the grant funds in preserving and creating jobs.

Our assessment strategy focuses on the scope of our activities and on the degree of detail to which we can report relevant metrics. Where breadth is concerned, our goal is to integrate the efforts of all stakeholders in a way that does not replicate measurement but instead emphasizes reliable and timely reporting of statewide metrics in a transparent way. This effort will include collaboration with individual providers seeking Meaningful Use incentives through Medicare and Medicaid, vendors, health care delivery organizations, quality improvement organizations, operational exchanges and our Regional Extension Center (REC) - the Louisiana Health Information Technology (LHIT) Resource Center. Examples of breadth metrics include the percentage of prescriptions filled electronically; the percentage of clinicians using HIE and EHRs; and the number of underserved regions, practices or individuals.

Where depth is concerned, our goal is to derive sufficient data on individuals—and through aggregation on the population—to measure meaningful impacts on care enabled by HIT. Examples of depth include timeliness and completeness of care transitions, adherence to medication regimens or complex disease management protocols, and the extent to which

individuals can contribute through PHRs, web-portals and other emerging consumer-focused technologies.

The ongoing assessment and evaluation of LaHIE will inform both the reporting requirements established under this funding opportunity and the care coordination and quality improvement goals of the HIE effort, which in many cases will be the same. We recognize that this effort will require information on providers, e.g., such as individual, facility, and EHR adoption/HIE participation status. We plan to utilize the LaHIE provider directory as the primary source of this information. The priority areas of assessment and evaluation are: a.) Laboratories participating in delivering electronic structured lab results; b.) Pharmacies participating in e-prescribing; and c.) Providers exchanging patient summary of care records along with proposed metrics.

### 3.3 Louisiana HIE Evaluation Framework

The following table represents the LaHIE Evaluation Framework. This framework will be modified and enhanced during the duration of the evaluation to meet the needs of the program.

The **Focus Areas** are the broad dimensions that LHCQF plans to measure through the evaluation efforts. These are:

- **Adoption/Utilization**
- **Effectiveness**
- **Barriers/Vulnerabilities**

Within each Focus Area, *Objectives/Strategies*, *Outcome Measures*, and *Impact Measures* have been described.

- *Objectives/Strategies* describe the objectives that we plan to accomplish relative to improving patient care, expansion of the HIE, and support of meaningful use.
- *Outcome and Impact Measures* are the metrics that will measure our progress and success towards these objectives. The LaHIE evaluation framework consists of a two-tier approach:
  - Tier One Outcome Measures are comprised of a number of quantitative metrics that can be obtained relatively easily.
  - Tier Two Impact Measures are a set of qualitative and quantitative assessments designed to delve deeper into the impact and success of LaHIE, as well as our effectiveness and success relative to managing grant funds to achieve desired outcomes.
- *Methods and Data Sources* detail the methods and data sources that will be used to obtain that data in order to evaluate whether we are meeting the listed measures.

<b>Louisiana HIE Evaluation Framework</b>				
<b>Focus Areas</b>	<b>Objectives/Strategies</b>	<b>Tier One: Outcomes Measures</b>	<b>Tier Two: Impact Measures</b>	<b>Methods and Data Sources</b>
<b>Adoption/Utilization</b>	Support the development and expansion of health information exchanges to improve the quality and efficiency of care.	By the end of 2012, the number of hospitals participating in LaHIE will increase from 4 to 35.	How many hospitals have joined in 2012?	The number of Participation Agreements and use of internal sources.
<b>Adoption/ Utilization Effectiveness</b>	Support the development and expansion of health information exchanges to improve the quality and efficiency of care.	By the end of 2012, the number of unaffiliated physicians using LaHIE will increase from 0 to 25.	<b>Provider satisfaction with HIE</b> <ul style="list-style-type: none"> <li>• Are providers satisfied with the ease of use and integration into their workflow?</li> <li>• Do providers feel that they are better able to provide care by having more complete patient information at the point of care?</li> <li>• Do they have concerns about HIE?</li> <li>• What improvements and/or enhancements would they like to see?</li> <li>• What are the characteristics of those</li> </ul>	2010 Environmental Scan

			not participating in HIE? Why did they choose not to participate? What would encourage them to participate?	
<b>Adoption/Utilization Effectiveness Barriers/Vulnerabilities</b>	Support the development and expansion of health information exchanges to improve the quality and efficiency of care.	LaHIE will track participation of long-term care facilities, pharmacists, dentists, home health providers, chiropractors, etc.	Percent of Long term care facilities, Pharmacists, Dentist, Home Health Providers, Chiropractors, etc. are participating in LaHIE from 2010.	2010 Environmental Scan
<b>Adoption/Utilization Effectiveness Barriers/Vulnerabilities</b>	Support the development of interconnections among health information exchanges in the state and nationwide.	The development of policies, procedures, and technical infrastructure to exchange data between LaHIE and Beacon.	Are the policies, procedures, and technical infrastructure to exchange data between LaHIE and Beacon in place?  Barriers to exchange?	LaHIE Policy and Procedures and Technical Infrastructure framework.
<b>Adoption/Utilization Effectiveness</b>	Support meaningful use. Support the development of interconnections among health information	Providers exchanging patient summary of care records.	Number or Percent of providers exchanging patient summary of care records.	Count the number or percent of providers exchanging patient summary of care record either through XDS or via

	exchanges in the state and nationwide.			Direct Secure Messaging.
<b>Adoption/Utilization Effectiveness Barriers/Vulnerabilities</b>	Support meaningful use.	The % pharmacies activated for e-prescribing will increase from 83.65% at the close of 2011 to 85.65% by the end of 2012	<p><b><u>E-Prescribing</u></b>                  What is the effectiveness or discrepancy rate between what was intended to be prescribed and what was dispensed?                  What are the vulnerabilities/causes behind the discrepancy rate?                  What efficiencies are gained by e-prescribing?                  How often are providers accessing patient medication history?                  How is the medication history helping with patient adherence/compliance?                  Does having access to formularies and eligibility information increase the usage of generics?</p>	2010 and 2012 Environmental Pharmacy Survey results.  2010 Environmental Scan
<b>Adoption/Utilization Effectiveness Barriers/Vulnerabilities</b>	Support meaningful use.	The number of labs exchanging electronic results through initial assessment was only 22%	<p><b><u>Labs</u></b>                  Has the rate of redundant diagnostic testing decreased since the implementation of HIE?</p>	2010 and 2012 Environmental Lab Survey results.

		of labs submit electronically.		
		Increase the number of Labs sending electronic lab results to providers in a structured format from 27.9% in 2011 to 40% by the end of 2012.	Has the number or percent of laboratories participating in delivering electronic structured lab results increased from the initial assessment in 2010 and the Environmental Lab Survey in 2012.	LaHIE and the 2010 and 2012 Environmental Lab Survey results Electronic Laboratory Reporting data from DHH
		Review LaHIE activity reports for health system to report on # of lab queries.	Are the participants using LaHIE for lab results?	LaHIE and the 2010 and 2012 Environmental Lab Survey results. 2010 Environmental Scan results.

<p><b>Adoption/Utilization Effectiveness</b></p>	<p>Support the development and expansion of health information exchanges to improve the quality and efficiency of care.</p>	<p>The use of LaHIE in the Emergency Department setting will increase in 2013.</p>	<p>What is the value of health information exchange in the emergency department?</p>	<p>2010 Environmental Scan results.</p>
<p><b>Effectiveness</b></p>	<p>Support the development and expansion of health information exchanges to improve the quality and efficiency of care.</p>	<p>Decrease the 30-day readmission rates in participating organizations.</p>	<p>Is there a decrease in re-hospitalization of patients associated with a single episode of care i.e. demonstrating reduction in the 30-day readmission rate?</p>	<p>Analytics</p>
<p><b>Adoption/Utilization/ Effectiveness Barriers/Vulnerabilities</b></p>	<p>Providers exchanging patient care summaries</p>	<p>The number of participants exchanging patient care summaries will increase</p>	<p><b><u>Care Summaries</u></b>                  Number or percent of providers using either Direct or XDS to exchange patient care summaries</p>	<p>2010 Environmental Scan Results</p>
<p><b>Adoption/Utilization Effectiveness Barriers/Vulnerabilities</b></p>	<p>Support meaningful use.                   Encourage the electronic exchange of public health data.</p>	<p>The number of providers electronically submitting data to the immunization registry will increase from 6 to 12 in 2012.</p>	<p><b><u>Public Health Exchange</u></b>                   Number or percent of providers submitting immunization data to the Immunization Registry.</p>	<p>2010 Environmental Scan Results                   Louisiana Immunization Network for Kids Statewide (LINKS)</p>

<b>Adoption/Utilization</b> <b>Effectiveness</b> <b>Barriers/Vulnerabilities</b>	Support meaningful use.  Encourage the electronic exchange of public health data.	The number of labs electronically submitting data to DHH will increase from 6 to 10 in 2012	Number or percent of labs electronically submitting data to DHH through LaHIE	LaHIE and the 2010 and 2012 Environmental Lab Survey results
--	---	---	---	--

### 3.4 Objectives for Obtaining Data

LaHIE will conduct a gap analysis focused on identifying gaps in the statewide availability of structured lab results delivery, e-prescribing, and sharing of clinical care summaries among unaffiliated organizations. The gap analysis will also evaluate the capacity of public health systems to accept electronic reporting of immunizations, notifiable diseases, and syndromic surveillance, as well as clinical quality reporting to Medicaid and Medicare.

LHCQF conducted a mail and electronic-based (online) Environmental Lab Survey in 2011 that included all CLIA Labs within the state of Louisiana to assess their availability, readiness, and use of electronic lab results, which did not yield enough effective data for analysis. Once we received more guidance from ONC to focus on the independent and hospital labs in Louisiana we initiated another survey to determine if the independent and hospital labs are operational and if they have the capability to send electronic results among other measures. After receiving the guidance from ONC, LHCQF is conducting its 2012 lab survey through direct contact with the nearly 485 independent and hospital lab providers in order to increase responses and capture more valuable data. We plan to have the results by the end of June 2012. In addition, LHCQF will facilitate open communications with LabCorp, Quest, and public labs about the percentages of orders being sent and received electronically.

As part of the 2010 Environmental Pharmacy Survey LHCQF collaborated with the State Board of Pharmacy and the Louisiana Independent Pharmacy Association to distribute surveys to independent pharmacies in Louisiana. The surveys were conducted in the same manner as the Lab Surveys. We plan to use phone contact to perform the 2012 survey to gather more valuable data. We plan to complete outreach by June 15, 2012 and have the results completed and reported by the end of Q2. With this survey we intend to validate if the pharmacy is still in business, is receiving eRx through another method, or needs additional information/education regarding e-prescribing. Through our efforts we have identified that there are 184 pharmacies at this time that do not have eRx capability according to Surescripts. LHCQF knows that addressing the white spaces revealed by the gap analysis will be a challenging yet important task. We will utilize the Louisiana Independent Pharmacy Association to encourage the adoption of eRx solutions among independent pharmacies. Through LaHIE, we will explore options to incentivize pharmacies to adopt new technology rather than continue to operate through hand written prescriptions and faxes. LHCQF will also explore options to create incentives for smaller labs to order and receive lab results directly through a provider's certified EMR.

In order to address the gaps identified and ensure stakeholder involvement, LHCQF will work with multiple stakeholder organizations through LaHIE to ensure that the white spaces for clinical care summary delivery are filled. All providers trying to meet Meaningful Use Stage 1 requirements will be given the means to do so through LaHIE. The NwHIN compatible Direct Secure Messaging and provider directory features will allow for this early exchange of the care summaries. LHCQF's Governance and Legal/Policy workgroups have completed the data use agreements and other necessary policies to ensure proper use of the secure messaging structure for Stage I of Meaningful Use. Through education, outreach and the services of the LHIT Resource Center, the providers are actively reached out to in order to acquire the ability to leverage the document exchange based on new technologies and workflows.

Once additional gap analysis is completed, LaHIE will use the data to develop strategies to address the identified gaps. These strategies will include direct provisions of services by LaHIE, leadership and direction through its multiple stakeholder structure, including the use of various policy and purchasing options that will be leveraged through the state. In addition, LaHIE will utilize services of other Louisiana Health Information Technology Resource Center (LHIT), stakeholder groups, and organizations to identify, reach out to, and assist providers in the gaps and white spaces. LaHIE will ensure that eRx, eLab, and electronic clinical care summary services necessary for Meaningful Use are available to all providers.

## 4. Privacy and Security Framework

### 4.1 Overview

In the Summer of 2010, the Louisiana Health Information Exchange (LaHIE) began developing a Privacy and Security Framework that aligns with the ONC Framework, as well as with the specifications developed for the Nationwide Health Information Network (NwHIN).<sup>3</sup> As required through its ONC grant, LaHIE is working to ensure that the HIE services are also consistent with federal policies and guidelines, and are based on technologies that are adaptable for future requirements, including exchange of information across state boundaries. As the entity for statewide health information exchange, LaHIE has developed privacy and security standards and protocols, as well as controls to ensure that they are implemented with fidelity. These policies and standards were applied at LaHIE pilot sites in November 2011, and are continuously refined based on feedback from the pilot sites. This plan describes the framework for those privacy and security standards, as well as the mechanisms required to ensure that participating organizations and individuals (health care providers, hospitals, payers, and patients) understand how these policies will be implemented within their respective domains.

The LaHIE Privacy and Security Framework mirrors the ONC framework, and incorporates the ONC's eight guiding principles in the Privacy and Security Framework: Individual Access & Correction; Openness and Transparency; Individual Choice; Collection, Use, and Disclosure Limitation; Data Quality and Integrity; Safeguards; and Accountability. These are described in further detail below.

Additionally, the Markle Foundation's *Connecting for Health Common Framework*<sup>4</sup> was used as reference material for this document. The Markle Common Framework contains nine Policy Principles that align with the ONC Framework's eight Principles, with a few exceptions.

### 4.2 Domain: Openness and Transparency

#### 4.2.1 Description of Approach and Corresponding Policies

The HIPAA Privacy Rule requires that participating organizations, with certain exceptions, must provide a notice of its privacy practices (NPP) to patients.<sup>5</sup> Aligned with the Privacy Rule, the ONC Framework Openness and Transparency Principle states that "There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information." Likewise, the Markle Common Framework relies on the same principle and adds that individuals should be able to know what

---

<sup>3</sup> The Nationwide Health Information Network (NwHIN) is being developed to provide a secure, nationwide, interoperable health information infrastructure that will connect providers, consumers, and others involved in supporting health and healthcare. When complete, it will connect regional HIEs together to provide universal access to electronic health records across jurisdictions and hospital systems, with expected benefits of safer treatments, greater operational efficiencies, lower risk, and, eventually, lower costs.

<sup>4</sup> "The Common Framework: Overview and Principles, The Markle Foundation, April 2006

<sup>5</sup> "Openness and Transparency," Privacy and Security Tiger Team Meeting, September 24, 2010.

information exists about them, the purpose of its use, who can access and use it, and where it resides.

LaHIE has no direct or indirect contact with patients, and thus requires that the duty of providing this notice reside with the participating organizations. The LaHIE policies and Participation Agreement are drafted to ensure that participating organizations provide this notice to all patients. The Participation Agreement is included as Appendix 7.1, and the LaHIE policies will be provided to all participants and interested parties.

According to HIPAA, the NPP must cover:

- Legally permitted uses and disclosures of protected health information (PHI)
- Duties to protect privacy
- Privacy practices, and abide by the terms of the current notice
- Patient's rights, including the right to complain to HHS and to the covered entity
- A point of contact for further information and for making complaints
- The NPP is not required to cover a summary of the actual uses and disclosures by the participating organization, but is optional, and may be used to highlight the disclosures and uses that are most relevant.

Providers with a direct treatment relationship with patients must distribute a privacy practices notice to patients by:

- Personal delivery (for first patient visits)
- Automatic and contemporaneous electronic response (for electronic service delivery)
- Prompt mailing (for telephonic service delivery)
- Posting the notice at each service delivery site in a clear and prominent place where patients seeking service may reasonably be expected to be able to read the notice
- Furnishing the notice as soon as practicable after an emergency treatment situations ends
- Supplying the notice to anyone on request
- Provider must also make its notice electronically available on any web site it maintains for customer service
- Provider with a direct treatment relationship with individuals must:
  - Make a good faith effort to obtain written acknowledgement from patients of receipt of the privacy practices notice
  - Document the reason for any failure to obtain the patient's written acknowledgement
- Provider is relieved of the need to request acknowledgement in an emergency treatment situation

Key considerations for ensuring openness and transparency revolve around the definition and handling of personal health information, or “protected health information” as it is termed in LaHIE. The ONC term is “individually identifiable health information.”

**Defining what is considered “protected health information”.** LaHIE considers PHI to be information that identifies a patient, provided to a participating organization in the Exchange, and can include and includes any part of an individual's medical record or payment history.

LaHIE mirrors the definition of protected health information as defined by the Health Insurance Portability and Accountability Act (HIPAA) Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subpart E, and the HIPAA Security Standards, 45 C.F.R. Part 160 and Part 164, Subpart C, both as amended from time to time.

**Identifying what PHI the participating providers collect.** As a conduit for the exchange of information among participants, LaHIE’s hybrid infrastructure model will store a minimum amount of health data centrally, primarily facilitating the secure transfer of health data between participating health care organizations that store the health data at their disparate locations. LaHIE will enable the exchange of data stored in existing provider networks while maintaining an option to store data centrally (e.g., smaller provider groups without their own database or network; or public health surveillance databases).

The above requirements are addressed in the LaHIE Policy **“Openness and Transparency Policy for Individually Identifiable Health Information”** and **“Access to LaHIE in accordance with HIPAA Privacy Rule.”**

#### 4.2.2 Description of Stakeholder Outreach

In the Summer of 2010, LaHIE convened a working group – the LaHIE Legal and Policy workgroup – to develop the policies, procedures, and legislative recommendations required to effectively and securely implement a HIE in Louisiana. This working group consisted of representatives from Louisiana hospital systems, the Louisiana Hospital Association, Louisiana’s Medicaid program, the Louisiana Department of Health and Hospitals, physicians, payers, the state nursing association and health care attorneys.

In addition to performing a review and analysis of state and national sources, especially HIPAA Privacy and Security Standards, LaHIE also sought input from surrounding states, communicating with HIE workgroups in those states as appropriate.

Following this process, LaHIE developed its privacy and security framework, which informed the development of the necessary agreements and policies and procedures required to effectively and securely implement a HIE in Louisiana. The agreements, policies and procedures were vetted through LaHIE’s stakeholder groups and reviewed by legal teams representing LaHIE connectors to ensure endorsement and adoption by health care providers and other stakeholders.

As these work products are considered living documents that will evolve, LaHIE, with continuous stakeholder involvement and input, will review and update the Policy Manual at least annually to comply with changes in the law, including relevant standards and implementation requirements of HIPAA and the State of Louisiana.

#### 4.2.3 Description of Gap Area

None.

### 4.3 Domain: Collection, Use and Disclosure Limitation

#### 4.3.1 Description of Approach and Corresponding Policies

The Collection, Use, and Disclosure Limitation Principle in the ONC Framework emphasizes that appropriate limits should be set on the type and amount of information collected, used, and disclosed, and that authorized persons and entities should only collect, use, and disclose information necessary to accomplish a specified purpose. The Markle Common Framework uses the same principle, and adds that the information should be obtained by lawful and fair means, and that patients should have the knowledge of or provide consent for collection of their personal health information.

The HIPAA Privacy Rule:

1. Generally requires covered entities to limit uses, disclosures, and requests of protected health information (PHI) to the minimum necessary (see *Minimum Use Standard* below); and
2. Defines and limits the uses and disclosures covered entities may make without an individual's authorization (see *Defining and Limiting Use and Disclosures* below).

#### **Minimum Use Standard**

The HIPAA Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of PHI to the minimum necessary to accomplish the intended purpose. In some cases, the Privacy Rule does not require that the minimum necessary standard be applied, such as, for example, to disclosures to or requests by a health care provider for treatment purposes, or to disclosures to the individual who is the subject of the information. LaHIE has developed reasonable policies and procedures to limit the information disclosed or requested on a routine/recurring and non-routine basis.

**Routine or recurring requests and disclosures:** LaHIE requires that its participating organizations implement reasonable policies and procedures (which may be standard protocols) to limit the information disclosed or requested. LaHIE has developed security measures (see *Safeguards Section*) to limit access through various means including portal encryption, single point of access, etc. Additionally, for routine exchanges of information for treatment purposes, LaHIE has developed a standard set of information that should be included in an exchange and that would be considered minimally necessary for the purpose. Doing so is consistent with the Collection, Use, and Disclosure Limitation Principle, and according to the U.S. Department of Health and Human Services, may help foster increased trust in electronic health information exchange.<sup>6</sup>

---

<sup>6</sup> "Health Information Technology - HIPAA Privacy Components of the *Privacy and Security Toolkit*; located at <http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/>

**Non-routine disclosures and requests:** LaHIE’s contract (the “Participation Agreement”) with participating organizations (also known as “business associates”) limits the business associate’s uses and disclosures of, as well as requests for, PHI to be consistent with LaHIE’s minimum necessary policies and procedures, since a business associate contract may not authorize the business associate to use or further disclose the information in a manner that would violate the Privacy Rule.

For electronic health information exchanges by a participating organization to and through LaHIE are subject to the minimum necessary standard, such as for a payment or health care operations purpose, the Privacy Rule would require that the minimum necessary standard be applied to that exchange and that the business associate agreement limit LaHIE’s disclosures of, and requests for, PHI accordingly.

### **Defining and Limiting Use and Disclosures**

The Privacy Rule defines and limits the uses and disclosures of PHI a covered entity may make without the individual’s authorization. In doing so, and consistent with the Collection, Use, and Disclosure Limitation Principle, the Privacy Rule defines the permitted uses and disclosures based on the purpose of the use or disclosure, and attaches conditions accordingly.

According to LaHIE policies (Policy “**Confidentiality and Security of Protected Health Information**”), the only permitted use of data is for treatment, coordination of care, and healthcare operations that promote efficiency of communication in care, patient safety, and enhance patient health. These are all allowable uses according to the Privacy Rule. Non-permitted uses of data include: third party services, services prohibited by state or federal law, comparative studies, underwriting, or marketing.

Regardless of the scope of the purposes for the electronic health information exchange environment, any disclosures by a HIPAA covered entity to or through a HIO must be in accordance with the Privacy Rule. Also, according to the Privacy Rule, participating organizations in LaHIE must have a business associate agreement with LaHIE that defines the uses and disclosures that LaHIE is permitted to make with PHI on a covered entity’s behalf. LaHIE has developed this business associate agreement.

The above requirements are addressed in the LaHIE Policy “**Confidentiality and Security of Protected Health Information**” and “**Compliance with Privacy and Security Laws and Protocol.**”

#### **4.3.2 Description of Stakeholder Outreach**

See Section 4.2.2 for description. In addition, LaHIE, as part of its Participation Agreement and onboarding process to the HIE, works with each participant to ensure all Privacy and Security measures are being followed. LaHIE works directly with the participants’ Privacy and/or Security officers on an ongoing basis to ensure compliance.

### 4.3.3 Description of Gap Area

None.

## 4.4 Domain: Safeguards

### 4.4.1 Description of Approach and Corresponding Policies

The ONC Framework and the Markle Common Framework assert that individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.

The Orion Health solution, which is the backbone of LaHIE, has been developed to include world-class privacy and security standards for effective health information exchange that protect the patient's right to privacy. LaHIE, in partnership with Orion Health, has developed administrative, technical, and physical safeguards to protect individually identifiable health information and minimize the risks of unauthorized or inappropriate access, use, or disclosure. These are outlined below.

**Single Point of Access.** The Orion Health HIE's single point of entry can be used as a secure, centrally controlled sign-on to multiple health information systems and data sources, eliminating the need for clinicians to manage multiple passwords. It can also integrate with peripheral authentication devices such as smart cards, biometric readers and proximity cards, avoiding the need for clinicians to remember a login and password.

**User Permissions:** The ability to access the HIE is based on the user's role as a participating organization. A user may be assigned to one or more user groups. In addition to belonging to multiple groups, users can be assigned to user groups that determine their level of access to different information systems. For example, clinicians, nurses and administrators would each require different levels of access to patient information. The membership, user privileges and restrictions of these access groups can be fully configured to suit the unique needs of each participating site. By default, access can be controlled based on user ID, user group, workstation location, and user's relationship to the patient. The solution offers the flexibility to extend these options into other areas, such as the facility where the user is based, or the user's specialty, department, or scope of practice.

Access can be limited in the following ways through the system, as outlined by LaHIE Policy "**User Permissions Policy**" and implemented through the system architecture:

- **No Access** – the patient's name will not be visible to the user in a work list or list of search results.
- **Locked** – the patient's name (demographic information) will be visible in a list of search results, but cannot be selected.

- **Privacy sealed** – the patient’s name will be visible and can be selected, but a reason for access will be required before the patient can be placed in context and their medical details viewed.
- **Full Access** – clinical users have unrestricted access to clinical data/documents in the patient’s medical record as they have a valid relationship with the patient and the patient has “opted-in”, i.e. chosen to have their information available in the HIE.

**Audit Trails:** All user activity within the system is logged, enhancing audit capabilities and improving the general security of patient data. Audit trails of user logins, logouts, applications used, security overrides, patient selections and individual documents viewed are recorded, with the date and time. Audit log data is stored in a separate audit database. (See “**LaHIE Audit Policy.**”)

**Electronic Encryption:** The HIPAA Privacy Rule allows covered health care providers, business associates and patients to communicate electronically, provide they apply reasonable safeguards when doing so. LaHIE will render personal health information unusable, unreadable, or indecipherable to unauthorized individuals for “data in motion” and for “data at rest.”<sup>7</sup> These industry standard encryption methods, including TLS and IP-SEC mechanism will ensure that unauthorized users are blocked from IIHI. The HIE utilizes industry standard encryption methods including TLS and IP-SEC.

**Consent Management:** Data within LaHIE are assigned to information categories, which in turn have an information access policy defined for them. This policy controls who can access the data, and the level of access they have. Policies can be based on a range of factors including the user’s group memberships and their defined clinical relationship to the patient involved. Documents and reports received by LaHIE can be automatically assigned to an information category based on data they contain. The LaHIE Clinical Portal, developed by Orion Health, enforces patient level consent through the use of configured relationships between the patient and Clinical Portal users, and an authorized administrator configures this within the Clinical Portal.

**Sensitive Information:** Access to sensitive information (such as HIV status) can be restricted, and is determined by each Participant. The LaHIE Clinical Portal controls access to modules using a role-based security model, based around the membership of individual users to one or more user groups. Groups are assigned access to applications, and it is an individual user’s group membership that determines the applications they can access. This means data can be masked at the user group level or individual user level. User access to data can be controlled to the field level using the dynamic patient summary view and configuring appropriate portlets. Sensitive patient health information, (e.g. HIV/AIDS, sexually transmitted diseases, substance abuse, mental health conditions), that is shared with LaHIE is still restricted from access for most purposes. This information can only be accessed with patient’s consent and under an “opening the privacy seal” access process and only by a clinician. See LaHIE Policy “**Information Subject to Special Protection.**”

---

<sup>7</sup> *Data in motion* refers to the transfer of that data between all these copies and versions of the original file, such as data traversing the Internet. *Data at rest* refers to data storage.

**Physical Safeguards:** LaHIE has policy in place to ensure that the HIE Exchange complies with the specific system security standards with respect to the Data Center. LaHIE is responsible for ensuring that all delivery and loading areas at the facility are restricted to prevent unauthorized access to its facilities. LaHIE will perform a periodic risk analysis in order to assess the level of physical access risk and adjust procedures accordingly. Additionally, LaHIE policy (“**Physical Security of Hardware, Data, Media and Equipment**”) requires that participating organizations ensure the physical security of the locations where authorized users access the Exchange and ensure compliance with HIPAA Privacy and Security requirements and all other applicable confidentiality laws and regulations. (Covered by LaHIE Policy “**Access to LaHIE in accordance with HIPAA Privacy Rule.**”)

#### 4.4.2 Description of Stakeholder Outreach

See Section 4.2.2 for description. In addition, LaHIE as part of its Participation Agreement and onboarding process to the HIE, works with each participant to ensure all Privacy and Security measures are being followed. LaHIE works directly with the participants’ Privacy and/or Security officers on an ongoing basis to ensure compliance.

#### 4.4.3 Description of Gap Area

None.

### 4.5 Domain: Accountability

#### 4.5.1 Description of Approach and Corresponding Policies

The ONC’s nationwide privacy and security principles will not be effective in building trust in electronic exchange of individually identifiable health information unless there is compliance with the above-referenced principles and enforcement mechanisms. The Markle Common Framework emphasizes that entities in control of personal health information must be held accountable for implementing these principles. The HIPAA Privacy Rule provides the foundation for accountability within an electronic health information exchange environment by requiring covered entities that exchange protected health information (PHI), whether on paper or electronically, to comply with its administrative requirements and extend such obligations to their business associates. The Privacy Rule also promotes accountability by establishing mechanisms for addressing potential non-compliance with privacy standards through a covered entity’s voluntary compliance, a resolution agreement and corrective action plan, or the imposition of civil money penalties, if necessary.

LaHIE has adopted the ONC Framework as its own, with modifications as necessary; consequently, LaHIE has developed mechanisms to address:

- Monitoring for internal compliance including authentication and authorizations for access to or disclosure of individually identifiable health information;
- The ability to receive and act on complaints, including taking corrective measures; and

- The provision of reasonable mitigation measures, including notice to individuals of privacy violations or security breaches that pose substantial risk of harm to such individuals.

### **Monitoring for Internal Compliance**

LaHIE has developed multiple methods and policies to address monitoring for internal compliance, including authentication and authorizations for access to or disclosure of individually identifiable health information. These are as follows:

- **Audit Process** LaHIE will conduct audits of participating organizations on a regular basis to ensure the Exchange is being used only for purposes authorized by the Participation Agreement and the Policy Manual, and that each individual who views the data through the Exchange is doing so in a manner consistent with the Participation Agreement and the Policy Manual. Responsibilities are outlined for LaHIE as well as for the participating organizations, including the audit process and reporting requirements. (Covered by LaHIE Policy “**Compliance with Privacy and Security Laws and Protocol**” and “**LaHIE Audit Policy**.”)
- **Training:** Participating organizations are responsible for training all of its authorized users on compliance with LaHIE policy, the HIPAA regulations, other applicable privacy laws and rules and the participant’s privacy and security policies. LaHIE training will focus on ensuring that in building and operating LaHIE, the focus is maintained on the welfare, safety and concerns of the patients. LaHIE will train identified “super users” in each participating organization, and the “super users” will then be responsible for deploying training for all of its Authorized Users. (See “**LaHIE Training Policy**.”)
- **Authorized User Agreement/Restricted Access:** Each participating organization will designate its authorized users. Authorized users will include only those individuals who require access to the Exchange to facilitate use of the data for a permitted use. (This is covered in the “**Authorized Users Information and Types**” policy.)
- **Discipline for Violations.** Each participating organization is responsible for its authorized users compliance with all applicable laws and regulations. As such, each participating organization shall be responsible for disciplining any of its authorized users who violate the terms of LaHIE policy, HIPAA or other applicable laws and regulations in accordance with its own policies and procedures and any guidelines that may be adopted by the LaHIE Advisory Committee.
- **Termination of Access:** LaHIE reserves the right to terminate (or cause the applicable participating organization to terminate) the access to the Exchange of any authorized user who violates the terms of LaHIE policy, HIPAA or other applicable laws and regulations.

### **Ability to Receive and Address Complaints; Corrective Action**

**Complaints:** LaHIE will adopt policies and standards for the investigation, resolution and reporting of patient complaints, security breaches or other concerns relating to compliance with the Participation Agreement, LHCQF’s Policies and Standards, and applicable laws and regulations (“Compliance Concerns”). LHCQF will provide notice to Participants, pursuant to LHCQF’s policy and as required by law or regulation, of any Compliance Concern related to

Participant's Authorized Users' use of LaHIE, and Participant will cooperate with LHCQF in its investigation of any Compliance Concern and corrective action.

**Corrective Action:** According to LaHIE policies "Accountability Principle in the Privacy and Security Framework," "Corrective Action Policy," and "LaHIE Audit Policy," if an audit reveals noncompliance, a corrective action plan must be submitted by the participant to the LHCQF Executive Management and its Legal Counsel. The Director of Health IT or his/her designee will make a recommendation on the corrective action plan to the Executive Management and its Legal Counsel as to whether a specified corrective action plan should be accepted as presented, be revised as per agreement reached at the Executive Management and its Legal Counsel meeting, or be rejected. If a corrective action plan is rejected, depending on the nature of the problem uncovered in the audit, the Executive Management and its Legal Counsel may vote to suspend access to the Exchange for either the Participant or one or more Authorized Users of such Participant until the problem is adequately addressed.

### **Mitigation Measures**

LaHIE has developed multiple methods and policies to provide for reasonable mitigation measures, including notice to individuals of privacy violations or security breaches that pose substantial risk of harm to such individuals.

**Privacy or Security Breaches - Notification:** LaHIE policy requires that any participating organization notify LaHIE of any instances of which it is aware in which the confidentiality of the PHI has been breached. Likewise, LaHIE must inform the participating organization of the same, should a breach occur, and swift contract termination is permitted to the participating organization should the breach not be cured within ten days. The participating organization is required to notify the affected individual(s) as required by HIPAA, with the assistance, if necessary, of LaHIE if the privacy and/or security breach involves more than one organization. (This is covered in LaHIE policies "Data Breach Notification;" "Security Breach Response Protocol.")

**Remedy of Breach:** Under the Privacy Rule, at 45 C.F.R. § 164.530(f), a covered entity must mitigate, to the extent practicable, any harmful effects that are known to the covered entity and that result from a use or disclosure of PHI in violation of its own privacy policies and procedures, or the Privacy Rule by the covered entity or its participating organizations. According to LaHIE policies ("Data Breach Notification" and "Security Breach Response Protocol"), participating organizations are responsible for immediately investigating and mitigating to the extent possible, any privacy and/or security breach that they become aware of relating to their Clinical Data Repository or the LaHIE, and for reporting any actual or potential breach to the COO for any needed investigation or mitigation. The policy outlines the process that the organization must undertake to report and remedy the breach.

## Participation Agreement

The Privacy Rule requires business associate agreements to contain satisfactory assurances that a business associate will adequately safeguard PHI. Some of the satisfactory assurances by a health information organization, such as LaHIE, HIO acting as a business associate include:

- LaHIE will not use or disclose PHI except as allowed by the agreement;
- LaHIE will implement reasonable and appropriate safeguards for PHI; and
- LaHIE will report any uses or disclosures of PHI that violate the agreement to the covered entity.

The above requirements are addressed in the LaHIE Policies “*Accountability Principle in the Privacy and Security Framework, ” Compliance with Privacy and Security Laws and Protocol*” and the “*Participation Agreement.*”

### 4.5.2 Description of Stakeholder Outreach

See Section 4.2.2 for description. In addition, LaHIE, as part of its Participation Agreement and onboarding process to the HIE, works with each participant to ensure all Privacy and Security measures are being followed. LaHIE works directly with the participants’ Privacy and/or Security officers on an ongoing basis. Additionally, all participants must sign business associate agreements that contain information regarding the accountability framework that all entities involved in LaHIE must conform to.

### 4.5.3 Description of Gap Area

None.

## 4.6 Domain: Individual Access and Correction

### 4.6.1 Description of Approach and Corresponding Policies

#### Individual Access

The ONC defines the Individual Access Principle as providing individuals with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format. The Markle Common Framework defines this assurance of access as the ability and means for individuals (patients) to *control* access to their personal information, and thus asserts that the individuals should have the *right* to have personal data relating to them communicated within a reasonable time and in a form that is readily understandable.

Through its policies and participation agreement, LaHIE is designed to ensure that individuals are provided with the means to access and obtain their individually identifiable health

information in the manner consistent with the ONC Framework and the Markle Common Framework.

The LaHIE system, as a conduit for most centralized data, recognizes that the individual medical record is the property of the participating organizations. Thus, the responsibility for ensuring the right of the individual to control access to personal data rests within each participating organization. At the same time, LaHIE operates on the belief, promoted by the Markle Common Framework, that:

*“.....individuals should be seen as key participants in processes of information collection and dissemination, and not as mere subjects or passive spectators. At all stages in the information chain, they should be able to inspect and query their information, and to determine who uses that information. In addition.....they should have clear avenues to correct information.”*

The LaHIE privacy protections related to individual access were designed with this principle in mind. Thus, each participating organization must agree, through the **LaHIE Participation Agreement, Individual Access to PHI**, and the **Confidentiality and Security of Protected Health Information Policy**, to ensure that patient health information is readily available to patients whenever it is requested.

Such control can be facilitated through the principles of transparency (previously discussed in the ***Openness and Transparency Domain***). In addition, personal information is collected directly from the individual rather than from a third-party. This enhances patient control over personal information. Finally, patients have meaningful opt-out clauses when they do not want their information to be reused, or when they want to “reclaim” their information.

## **Correction**

The HIPAA Privacy Rule provides individuals with the right to have their protected health information (PHI) amended in a manner that is fully consistent with the Correction Principle in the Privacy and Security Framework. (45 C.F.R. § 164.526.) The ONC Framework defines as the Correction Principle as the ability of the HIE to provide individuals with access to a timely means to dispute the accuracy or integrity of their individually identifiable health information, and to have erroneous information corrected or to have a dispute documented if their requests are denied. The Markle Common Framework echoes this principle, and further adds to it, stating that *“Individuals should have the right to be given reasons if a request is denied and to be able to challenge such denial.”*

According to the ***LaHIE Participation Agreement***, corrections to data are the sole responsibility of the participating organizations. Before they are granted access to LaHIE, participating organizations must agree to promptly correct any errors discovered in the data it transmits to LaHIE, and must notify the LHCQF in writing of any such corrections pursuant to LHCQF’s Policies and Standards.

The above requirements are addressed in the LaHIE Policies **“Correction Policy,”** and **“Individual Access to PHI.”**

#### 4.6.2 Description of Stakeholder Outreach

See Section 4.2.2 for description. In addition, LaHIE, as part of its Participation Agreement and onboarding process to the HIE, works with each participant to ensure all Privacy and Security measures are being followed. LaHIE works directly with the participants’ Privacy and/or Security officers on an ongoing basis.

#### 4.6.3 Description of Gap Area

None.

### 4.7 Domain: Data Quality and Integrity

#### 4.7.1 Description of Approach and Corresponding Policies

The ONC Framework recognizes that the completeness and accuracy of an individual’s health information may affect, among other things, the quality of care that the individual receives, medical decisions, and health outcomes. The Data Quality and Integrity Principle states that *“Persons and entities should take reasonable steps to ensure that individually identifiable health information is complete, accurate, and up-to-date to the extent necessary for the person’s or entity’s intended purposes and has not been altered or destroyed in an unauthorized manner.”* Likewise, the Markle Common Framework states that *“all personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and current.”*

In its role as an information conduit, LaHIE does not possess any original health data/individually identifiable health information. A participating organization is the repository of the original health data and therefore is the only entity that has the ability to validate the data with their source system. Therefore, the responsibility for ensuring that individually identifiable health information is accurate, complete, and up-to-date falls to participating organizations and patients. Per LaHIE Policy, the participating organizations must be responsible for validating the data.

In order to facilitate compliance with these requirements, the LaHIE has developed policy and procedures to detect, prevent, and mitigate any unauthorized changes to, or deletions of, individually identifiable health information, and has ensured that the process outlined is not unwieldy or inaccessible. If a data record requires a change, the process for making the change is simple and straightforward. Likewise, if a record change is not appropriate, there should be safeguards to prevent the alteration of the record.

LaHIE is bound by its policies to provide the mechanisms for data validation to occur. First, the LaHIE ensures that patient matching across providers is accurate as by design, LaHIE consolidates multiple medical records from multiple sources to provide a comprehensive, longitudinal view of a patient’s medical history. LaHIE has an Enterprise Master Patient Identity Management system built into its application. LaHIE’s identity management team works closely with participating partners to confirm patient matches. (See LaHIE Policy “**Enterprise Master Patient/Person Index Maintenance.**” Second, LaHIE ensures that the participating organizations are performing the data validation as part of their compliance requirements of HIPAA privacy and security and as part of the Participation Agreement terms. Finally, LaHIE will conduct annual privacy and security audits, per LaHIE policies “**Compliance with Privacy and Security Laws and Protocol**” and “**LaHIE Audit Policy.**”

Related to the *Individual Access* principle, individuals will also be able to ensure that information is being used for the originally stated purpose, and they will be able to correct errors in context as well as content. This requires that people be able to view not only what information exists on them, but also how it is being used. This is accomplished through the “**Individual Access to PHI Policy.**” which outlines the relationship of LaHIE with their partners in ensuring that the individual’s information is corrected/amended as appropriate. However, since LaHIE does not possess any original health data/individually identifiable health information, the participating organization is the only entity that has the ability to correct any errors in the context as well as content of the original health data

The above requirements are also addressed in the LaHIE Policy “**LaHIE Data Quality and Integrity.**”

#### 4.7.2 Description of Stakeholder Outreach

See Section 4.2.2 for description. In addition, LaHIE, as part of its Participation Agreement and onboarding process to the HIE, works with each participant to ensure all Privacy and Security measures are being followed. LaHIE works directly with the participants’ Privacy and/or Security officers on an ongoing basis.

#### 4.7.3 Description of Gap Area

None.

## 4.8 Domain: Individual Choice

### 4.8.1 Description of Approach and Corresponding Policies

The ONC Framework for the Individual Choice Principle states that “*Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information.*” The Markle Common Framework goes further to state that the purposes for which personal data are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes.

Patient control over health information, as well as security of confidential records, are key concerns in implementing an HIE. LaHIE has used the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as a guide for the design of the HIE system. HIPAA does not require any patient consent or authorization for the exchange of individual patient’s health information among health care providers for treatment purposes. A patient’s consent to such exchanges is viewed as implicit in the patient’s consent to receive medical care. Certain other exchanges are also permitted without either consent or authorization under HIPAA, generally for payment purposes and for certain health care operations. In addition, HIPAA permits disclosures to government agencies for a number of lawful purposes, including public health surveillance without patient consent or authorization. Other disclosures will require patient specific authorization (which the patient can withhold) in a form that meets the requirements of HIPAA.

In December of 2008, the Office of Civil Rights of the Department of Health and Human Services, the HIPAA civil enforcement arm of the Department of Health and Human Services, issued a series of related papers on the HIPAA Privacy Rule and Health Information Technology (the “Guidance”).<sup>8</sup> The Guidance constitutes an overview of HHS’ positions on the application of the HIPAA Privacy Rule to electronic health information exchanges. In general, the Guidance is consistent with, and supportive of, LaHIE —treatment purpose focused and with the HIE as a conduit for the exchange of information among participants. While recognizing that patients’ consent to the exchange of their information among health care providers for treatment purposes is implied in the general consent to be treated and does not require specific affirmation by the patient, the guidance favors allowing individuals the opportunity to opt-in or to opt-out of having their information flow through the HIE. The Guidance refers in this regard to the option providers are given in the HIPAA Privacy Rule to seek patient consent for treatment uses and disclosures, even in the absence of a requirement that providers do so. In addition, the Guidance affirms that an HIE, as a business associate, can maintain a master patient index (MPI) and a registry for patients of participating providers, in advance of any actual treatment communications for those patients.

It was identified that Louisiana is considered an “opt-in” state after thorough review of the Louisiana legislation. This means that a patient’s consent is explicitly required for his/her information to be accessed via LaHIE. If the consent has not been obtained and the patient

---

<sup>8</sup> HIPAA Privacy Rule and Health Information Technology (HIT), posted on the website of the Office of Civil Rights on December 15, 2008.

presents in an emergency situation, his/her information may be accessed in LaHIE for emergency treatment purposes only. If a patient explicitly opts out of LaHIE, his/her information cannot be accessed, regardless of any emergency situation. After connecting to LaHIE, providers/hospitals are required by LaHIE policy to include language in their respective privacy policies that references the exchange of health information through LaHIE. These requirements are covered in LaHIE Policy “***Individual Choice for Sharing Information in LaHIE.***”

#### **4.8.2 Description of Stakeholder Outreach**

See Section 4.2.2 for description. In addition, LaHIE, as part of its Participation Agreement and onboarding process to the HIE, works with each participant to ensure all Privacy and Security measures are being followed. LaHIE works directly with the participants’ Privacy and/or Security officers on an ongoing basis.

#### **4.8.3 Description of Gap Area**

None.



		Procedures Advanced Directives SSO Launching of the HIE Portal XDS Exchange DHH Points of Integration Immunizations bi-directional Syndromic Surveillance Electronic Lab Reporting Medicaid Eligibility verification GNOHIE Connection to LaHIE (Beacon) Automated Consent via Messaging
<b>HIE Implementation – Phase III Planning</b>		
January – August 2012	8 mo.	Analytics Requirements and Selection Interstate Exchange (NwHIN)
<b>HIE Implementation - Phase III</b>		
September 2012 – April 2013	8 mo.	Analytics Implementation Connect to NwHIN Quality Reporting Patient Access to LaHIE

## 5.2 Updated Staffing Plan

### **Staffing Changes**

Although the overarching governance model has not changed since the submission of the original Strategic and Operation plan, there have been changes made to the staffing plans (referenced in page 36 and detailed on page 92), and to LaHIE’s organizational structure (page 39). The changes to both areas are outlined below.

In the original Strategic and Operational plan, there were **4.3 FTEs**. LHCQF currently has **9.3 FTEs** to manage the operations and implementation of LaHIE. Subject Matter Experts (SME), consultants or contract employees are utilized as needed for specific functions. Key functional roles now include:

**Executive Director (0.3 FTE):** This position serves as the chief executive officer of the LHCQF. The position serves as the liaison with the Board of Directors to provide direction, oversight, strategic guidance and leadership for the HIE initiatives. (Included in Strategic and Operational plan)

**Director of Health IT (1.0 FTE, with 0.5 FTE budgeted to REC and 0.5 budgeted to LaHIE):** This position remains at .5 FTE as originally proposed. However, the sharing of this position with REC means that this individual is positioned to take advantage of any synergies that might exist between HIE and REC. The Director of Health IT provides executive-level leadership for LaHIE and oversees all HIT operations within LHCQF including HIE and REC projects. This position oversees all project development; draft, negotiate, manage and reconcile contracts with strategic partners; manage project staffs; and works with legal counsel on contracts. Both the Director of HIT and the Program Manager communicate with ONC, the State HIT Coordinator, and Beacon to coordinate HIE activities on an ongoing basis. (Included in Strategic and Operational plan)

**HIT Program Manager (1.0 FTE, with 0.5 FTE budgeted to REC and 0.5 budgeted to LaHIE):** This position serves as project director for the LaHIE initiative, and is responsible for the strategic and operational activities of LaHIE. The position utilizes the HIT Advisory Council to obtain key input regarding the direction and strategy of the LaHIE initiative. The HIT Program Manager is accountable for monitoring the program’s ongoing progress, communicating items for resolution to the Director of HIT and the HIT Advisory Council, and tracking the reporting requirements of the cooperative agreement to ensure timely and accurate completion. (NOTE: This position was included in the original Strategic and Operational plan, with the same .5 FTE time equivalent.)

**HIE Project Coordinator (1.0 FTE):** This position is responsible for the development and management of various projects and/or phases required for the implementation of the LaHIE initiative. (Included in Strategic and Operational plan)

**Business and Technical Operations Manager (1.0 FTE):** This position is responsible for the daily operations of the HIE and serves as the point person for technical architecture of LaHIE.

The position is responsible for the onboarding and training of HIE Participants and will also assure the security and integrity of the technical environment and data managed by the LaHIE initiative.

**Administrative Assistant (0.5 FTE):** This position is responsible for managing the front office, answering phones, ordering office supplies and providing clerical support and assistance to the HIT staff. (Included in Strategic and Operational plan, increased from 0 FTE)

**Business Manager/Contract Compliance (0.5 FTE):** This position is responsible for the day-to-day handling of LaHIE's financials, accounts receivables and contract billing. This position is also responsible for ensuring compliance with all deliverables of HIE grant and contracts.

**LaHIE Client Services Manager (1.0 FTE):** This position is responsible for outreach, business development and sales of the health information exchange to the health care community in Louisiana. This position will raise awareness and enthusiasm within the state for the HIE, explaining the benefits of participation as a data provider and/or user to the health care providers and payers as well as ensure continued customer service relationships with the data providers/users.

**LaHIE Client Executive (1.0 FTE):** This position is responsible for outreach, business development and sales of the health information exchange to the health care community in Louisiana. This position will raise awareness and enthusiasm within the state for the HIE, explaining the benefits of participation as a data provider and/or user to the health care providers and payers as well as ensure continued customer service relationships with the data providers/users.

**HIE Technical/System Integrations Specialist (1.0 FTE):** This position serves as a HIE technical specialist for LaHIE as well as a system integrations specialist for providers to access LaHIE. (Included in Strategic and Operational plan)

**HIE Operations Specialist (1.0 FTE):** This position serves as the HIE operational analyst/specialist for LaHIE providing onboarding and training assistance to the HIE Participants. In addition, this position is responsible for ensuring that the Enterprise Master Person Index (EMPI) is maintained and accurate as well as ensuring all LaHIE policies and procedures are thoroughly documented and maintained.

**HIT Accounting Coordinator (1.0 FTE; position is currently budgeted in REC but will transition to HIE in 2014):** This position is responsible for the day-to-day handling of LaHIE's accounts receivables and contract billing.

**Marketing and Communications Director (0.5 FTE):** This position is responsible for the development, implementation and evaluation of marketing and communication strategies and materials for the health information exchange in Louisiana. (Included in Strategic and Operational plan, increased from 0 FTE, was originally a coordinator)

**Human Resources:** This function is currently outsourced. The function is responsible for payroll, employee benefits, employee hiring/retention/counseling/coaching, policies and procedures and HR compliance.

**Financial Management:** This function is currently outsourced and is responsible for managing LaHIE’s financial risk, financials, budgets, AR/AP, investments, audits, financial analysis and cost accounting.

**Legal:** This function is currently outsourced and is responsible for assuring that all legal aspects regarding the implementation and operation of the health information exchange are identified and addressed.

**Tier 1 Support:** This function is outsourced and is responsible for ensuring all Tier 1 Help Desk support for LaHIE is provided in a timely and efficient manner.

**Proposed Additional Staffing**

**HIE Project Coordinator (1.0 FTE):** See description above. As the number of participants increases and LaHIE matures, it is anticipated that additional resources will be needed for maintaining and growing the exchange. Adding this position would provide the project with two Project Coordinators.

**LaHIE Client Executive (1.0 FTE):** See description above. It is anticipated that additional resources will be needed as LaHIE matures and the number of participants increases. These resources will allow us to continue providing full time customer service to the clients. Adding this position would provide the project with two Client Executives.

**Budget Implications of Proposed Changes:**

The budget implications are summarized in the table below. The original values are found in page 95 of the SOP.

	2011	2012	2013	2014	2015	2016
<b>Original Salaries and Benefits</b>	\$373,136	\$386,825	\$402,297			
<b>Original Contractual Costs</b>	\$2,248,175	\$737,839	\$826,127			
<b>Updated Salaries and Benefits</b>	\$885,290	\$1,163,405	\$1,209,941	\$998,448	\$1,038,386	\$1,079,921
<b>Updated Contractual Costs</b>	\$227,415	\$200,000	\$200,000	\$200,000	\$200,000	\$200,000
<b>Difference (updated-original)</b>	<b>\$(1,508,606)</b>	<b>\$238,741</b>	<b>\$181,517</b>	<b>\$1,198,448</b>	<b>\$1,238,386</b>	<b>\$1,279,921</b>

**Updated Organizational Chart:**

The updated organizational chart is found in Appendix 7.3.

### 5.3 Updated Discussion of Risks and Mitigation Strategies

In addition to the risks listed in the original Strategic and Operational Plan (page 86), the following risks and mitigation strategies have been identified and categorized into external and internal risks, along with their respective mitigation plans.

#### 5.3.1 External Risks

**Risk:** The rapid evolution of HIE approaches and mechanisms may pose the greatest risk. Many states are focusing their efforts on required services. LaHIE shares the belief that HIE is largely a matter of coordinated services, but an HIE organization cannot be assured to have a monopoly on services. Many of the early Nationwide Health Information Network (NwHIN) activities (2005-2006) are now available through a range of competing interests. These include medication information, eligibility, laboratory reports, and secure messaging. As Internet-based technologies and NwHIN approaches evolve, these services are expected to increase.

- **Mitigation of risk:** Remain flexible, and respond to user demand. Proactively work with stakeholders to identify valuable service offerings and successfully implement them in a timely manner.

**Risk:** Demand is lower than anticipated, and payer and provider participation is low.

- **Mitigation of risk:** Develop marketing and communications plan and monitor and refine continuously. Proactively identify barriers to adoption and address those issues quickly.

**Risk:** Changes in the legal and regulatory landscape.

- **Mitigation of risk:** Continually monitor the legal and regulatory landscape working closely with legal counsel, DHH and appropriate parties to assess options.

**Risk:** Mature integrated delivery networks (e.g., Ochsner, FMOL, LSU, etc.) that have already invested millions of dollars to achieve meaningful use may see little value in HIE capabilities.

- **Mitigation of risk:** Proactively work closely with the large integrated health systems to understand their current capabilities and plans for HIE capabilities. Provide clear and meaningful capabilities enabling those organizations to obtain value added benefits by participating in Statewide HIE and also link to Federal HIE initiatives. Work with the executive staff in these organizations to link the HIE to their strategic goals and engage them via participation in the Advisory Committee. Offer early adopter incentives.

**Risk:** Opt-in consent model may not be viable.

- **Mitigation of risk:** Work closely with legal counsel to assess options. Work with the State of Louisiana to educate legislators on the benefits of HIE and why they should support an opt-out model.

**Risk:** The vendor doesn't deliver as promised.

- **Mitigation of risk:** Monitor the detailed implementation plan and Statement of Work with Orion that includes clear milestones, timelines, roles and responsibilities. A vendor management plan has been developed to identify and mitigate any potential risks. Be prepared to supplement Orion resources with other technical support on a contingency

basis, as needed. Conduct frequent status meetings/calls among LaHIE, early adopter organizations and Orion. Rapidly escalate any issues or problems within Orion to senior leadership. A contingency plan will be put in place to address any failures by the vendor to fulfill their requirements. If Orion doesn't fulfill its contractual obligations, as outlined per the contract, Orion is required to provide transition assistance to LaHIE for no less than six months and no more than twenty-four months to ensure transition of their data and processing capabilities to a successor HIE system.

**Risk:** Vendor may be acquired by a larger firm.

- **Mitigation of risk:** Monitor industry developments and any potential acquisition. If an acquisition occurs, meet immediately with the acquiring entity's senior management and gain commitment for continued support per the vendor's contract and verbal commitments.

**Risk:** HIE competitors within the state.

- **Mitigation of risk:** LaHIE will work with other HIEs in the state to leverage/maximize resources and capabilities. Where true competition arises, LaHIE will ensure continued delivery of valuable services at reasonable fees. Rapid deployment and achieving critical mass with major players (health systems and payers) will establish LaHIE as the *de facto* HIE for the State.

**Risk:** Federal or state funding not available.

- **Mitigation of risk:** Implement the sustainability plan (see Section 8) to reduce or eliminate reliance on public sector funding. Ensure multiple sources of funding (provider, payer, state, employers and other health care stakeholders) to reduce reliance on government grant funding.

**Risk:** Market is larger than anticipated.

- **Mitigation of risk:** Develop a scalable system that can adjust to changes in demand, at minimal cost without sacrificing quality. Line up additional delivery/technical resources to allow LaHIE to quickly flex up with demand, without having to hire full time staff.

**Risk:** EHR vendors are not ready to connect.

- **Mitigation of risk:** Monitor industry developments and readiness. LaHIE will work with EHR vendors along with the LHIT Resource Center to rapidly escalate EHR vendor readiness concerns.

### 5.3.2 Internal Risks

**Risk:** Coordination among the many participating entities will be a major challenge to this work and failure to coordinate effectively will pose a risk to the project.

- **Mitigation of risk:** The Forum has been successful at bringing the major health systems, health insurers, and regional health information organizations (RHIOs) to the table for the planning process. As this continues, LaHIE will document commitments from these entities through contracts, data sharing agreements, and more. LaHIE will also continue its proven processes for stakeholder engagement and buy-in.

**Risk:** Costs are greater than anticipated.

- **Mitigation of risk:** Establish flexible pricing for LaHIE and set expectations with customers regarding how and when LaHIE pricing might change.

**Risk:** Organizational capacity is stretched as demand grows.

- **Mitigation of risk:** The Forum will engage consultants, contractors, and/or additional staff should the core team not have the capacity to handle the demand.

## 6. Tracking Program Progress

Program Priority	Report in first SOP update		Report January, 2013		Report January, 2014	
	Status as of December, 2011	Target for December, 2012	Status as of December, 2012	Target for December, 2013	Status as of December, 2013	Target for End of Grant Period
<b>1. % of pharmacies participating in e-prescribing</b>	84.3%	97%				
<b>2. % of labs sending electronic lab results to providers in a structured format</b>	27.97%	40%				
<b>3. % of labs sending electronic lab results to providers using LOINC</b>	<i>Baseline to be established in 2012</i>	<i>Baseline to be established in 2012</i>				
<b>4. % of hospitals sharing electronic care summaries with unaffiliated hospitals and providers</b>	19.18%	35%				

Program Priority	Report in first SOP update		Report January, 2013		Report January, 2014	
	Status as of December, 2011	Target for December, 2012	Status as of December, 2012	Target for December, 2013	Status as of December, 2013	Target for End of Grant Period
<b>4a. % of hospitals sharing electronic care summaries with hospitals outside their system (AHA)</b>	13.47%	20%				
<b>4b. % of hospitals sharing electronic care summaries with ambulatory providers outside their system (AHA)</b>	15.65%	35%				
<b>5. % of ambulatory providers electronically sharing care summaries with other providers</b>	19.22%	40%				
<b>6. Public Health agencies receiving ELR data produced by EHRs or other electronic sources. Data are received using HL7 2.5.1 LOINC and SNOMED.</b>	Yes	Yes				
<b>Yes/no or %</b>						

Program Priority	Report in first SOP update		Report January, 2013		Report January, 2014	
	Status as of December, 2011	Target for December, 2012	Status as of December, 2012	Target for December, 2013	Status as of December, 2013	Target for End of Grant Period
<p><b>7. Immunization registries receiving electronic immunization data produced by EHRs. Data are received in HL7 2.3.1 or 2.5.1 formats using CVX code.</b></p> <p>Yes/no or %</p>	Yes	Yes				
<p><b>8. Public Health agencies receiving electronic syndromic surveillance hospital data produced by EHRs in HL7 2.3.1 or 2.5.1 formats (using CDC reference guide).</b></p> <p>Yes/no or %</p>	Yes	Yes				
<p><b>9. Public Health agencies receiving electronic syndromic surveillance ambulatory data produced by EHRs in HL7 2.3.1 or 2.5.1.</b></p> <p>Yes/no or %</p>	No	No plans for this				

## **7. Appendices**

## **7.1 LaHIE Participant Agreement**

**LOUISIANA HEALTH INFORMATION EXCHANGE**

**MASTER PARTICIPATION AGREEMENT**

This Participation Agreement is entered into between Louisiana Health Care Quality Forum (“Quality Forum”) and the following Participant:

**Participant/Facility:**

**NPI Number (if applicable):**

**Address:**

**City/State/Zip:**

**Key Contact:**

**Email:**

**Phone:**

**Fax:**

**Signed Contract Date:** \_\_\_\_\_

**Effective Go Live Date:** \_\_\_\_\_

Where applicable, this Agreement also includes the following facilities owned by Participant, each and all of whom shall be individually bound as a Participant:

**Participant/Facility**

**NPI Number (if applicable):**

**Address:**

**City/State/Zip:**

**Key Contact:**

**Email:**

**Phone:**

**Fax:**

**Participant/Facility**

**NPI Number (if applicable):**

**Address:**

**City/State/Zip:**

**Key Contact:**

**Email:**

**Phone:**

**Fax:**

**Participant/Facility:**

**NPI Number (if applicable):**

**Address:**

**City/State/Zip:**

**Key Contact:**

**Email:**

**Phone:**

**Fax:**

**Participant/Facility**

**NPI Number (if applicable):**

**Address:**

**City/State/Zip:**

**Key Contact:**

**Email:**

**Phone:**

**Fax:**

## **BACKGROUND**

A. In 2009, Congress passed the Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”) as part of the American Recovery and Reinvestment Act of 2009 (the “ARRA”), to stimulate and promote the widespread adoption, standardization and electronic sharing of healthcare information across computerized networks and amongst multiple healthcare providers.

B. The Louisiana Health Care Quality Forum (“Quality Forum”) is a Louisiana non-profit corporation that has been appointed as the State-Designated Entity for Louisiana to lead in the planning and implementation of the health information technology grants provided through the ARRA for the establishment of an electronic health information exchange in Louisiana. As such, Quality Forum has entered into agreement with a third party software vendor that may be replaced by the Quality Forum as it deems necessary or appropriate (hereafter referred to as the “Current Software Vendor”), Orion Health, Inc., (“Orion”), to develop and maintain the Louisiana Health Information Exchange, (“LaHIE”), an Internet-based system that allows the secure exchange of electronic health information.

C. Quality Forum and Participant acknowledge and agree that the Quality Forum has worked extensively with the HIT Steering Committee, which consists of representatives from a number of Louisiana Health Care Providers that anticipate signing as Participants in LaHIE, in collectively drafting and jointly developing this Agreement.

## **AGREEMENT**

### **1. DEFINITIONS**

1.1 In this Agreement, capitalized words have the following meaning.

(a) “Authorized User” means an individual authorized by the Forum and/or a Participant pursuant to this Agreement to access and use LaHIE to input and/or access Data for a Permitted Use and who has signed an Authorized User Agreement in the form set forth in Exhibit B.

(b) “Business Day” means Monday to Friday 8am – 5pm, excluding public holidays.

(c) “Data” means protected health information, or information that identifies a patient that is entered into or made accessible to LaHIE by and/or on behalf of an authorized Participant and/or Authorized User. For purposes of this Agreement, protected health information is defined by the Health Insurance Portability and Accountability Act (“HIPAA”) Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subpart E, and the HIPAA Security Standards, 45 C.F.R. Part 160 and Part 164, Subpart C, both as amended from time to time.

(d) “Data Exchange” means electronically providing, communicating, entering, sharing, exchanging, supplementing and/or extracting Data through LaHIE.

- (e) "Effective Date" means the date entered on page 1 of this Agreement. In the event no date is entered on page 1, the Effective Date shall be the last of the dates entered on the signature page hereof.
- (f) "Health Care Provider" means a physician, group practice, hospital or health system, or other health care organization or professional that provides treatment and/or other health care services to Patients and has entered into a Participation Agreement with Quality Forum.
- (g) "LaHIE" is the Internet-based technology system developed, implemented and maintained by Quality Forum through the Current Software Vendor by which Participants and Authorized Users will be enabled to access, use and share Data.
- (h) "ONC" means Office of National Coordinator for Health Information Technology
- (i) "Participant" means a hospital, physician, entity or other Health Care Provider that has entered into a Participation Agreement with Quality Forum, including the Participant named as a party to this Agreement.
- (j) "Participation Agreement" means an agreement between the Quality Forum and a Participant which sets forth the terms and conditions pursuant to which the Participant will be authorized to access and use LaHIE.
- (k) "Patient" means an individual who has received or will receive treatment or health care services from a Health Care Provider.
- (l) "Permitted Use" means authorized use of LaHIE by Participants and Authorized Users for Data Exchange, including any other use that may be expressly documented in the Supplemental Terms attached as Exhibit F.
- (m) "Technical Environment" means the minimum hardware and software configuration or interfaces identified that Participant must have to be able to access and use LaHIE.
- (n) "Role Based Access Principles" means access decisions by Participant that are based on the roles that individual Authorized Users have as part of their respective duties towards or on behalf of Participant. Authorized Users take on assigned roles.
- (o) "Saas Service" means the specialized software that Orion has developed as part of its Software as a Service concept and has specially configured to form LaHIE and make it available to the Quality Forum and its Participants as a hosted application over the Internet.
- (p) "Term" means the period of time described in Section 10 below.

The following exhibits are incorporated into and made a part of this Agreement:

- Exhibit A - Security Requirements;
- Exhibit B – Sample Authorized User Agreement;
- Exhibit C - Business Associate Agreement;
- Exhibit D - Access Fees;
- Exhibit D-1 – Participant Fee Schedule
- Exhibit E – Technical Environment
- Exhibit F – LaHIE Features & Functionalities
- Exhibit G - Supplemental Terms.

## 2. **LICENSE TO ACCESS LAHIE FOR PERMITTED USE**

2.1 **Right to Use LaHIE.** Quality Forum grants to Participant for the Term of this Agreement a non-exclusive, nontransferable, non-assignable, non-sub-licensable, and limited right to access and use LaHIE pursuant to the terms of this Agreement for any Permitted Use. LaHIE shall not be used for any other purpose whatsoever, and shall not otherwise be copied or incorporated into any other computer program, hardware, firmware or product. LaHIE and any and all software and technology related thereto is licensed “as is.” Participant acknowledges that LaHIE and its corresponding technology has been licensed to Quality Forum by the Current Software Vendor, and that the license granted under this Agreement is subject in every respect to licensed rights granted to Quality Forum pursuant to the Software Vendor Agreement. As additional software and technology (collectively “Revisions”) is developed by or on behalf of the Quality Forum for use in connection with LaHIE, Participant agrees that all such Revisions shall automatically become subject to this Agreement and any use of said Revisions shall be subject to all terms and conditions of this Agreement. This Section 2.1 applies only to software, technology and/or Revisions that are provided or made available to Participant as part of LaHIE and not to any other software that Participant may use in providing treatment to Patients or for Participant's business operations. In the event any Revision is reasonably anticipated to cause any materially adverse impact or material increase in costs to Participant, Quality Forum will give reasonable notice to Participant of any material adverse impact or material cost increase known to Quality Forum prior to installation of the Revision and Participant will have 30 days from such notice to terminate this Agreement if Participant so desires.

2.2. **No Other Licensed Rights.** Any use of LaHIE not expressly permitted by this Agreement is prohibited.

2.3 **No Transfer or Modification.** Participant will not sell, rent, assign, sublicense or otherwise share its limited right to access and use LaHIE. Participant will not modify, reverse engineer, decompile, disassemble or otherwise attempt to learn the source code, structure or ideas upon which LaHIE, or any of its software or related technology, is based.

### 3. **QUALITY FORUM'S OBLIGATIONS**

3.1 **Access to LaHIE for Permitted Use.** Quality Forum will enable Participant and Authorized Users to access and use LaHIE for the Permitted Use specifically granted to Participant pursuant to section 2.1. Forum may establish arrangements with other health information exchanges to allow access to additional Data for a Permitted Use. Any change to a Permitted Use must be documented in a written amendment and signed by Quality Forum and Participant.

3.2 **LaHIE Availability.** Quality Forum will make commercially reasonable best efforts to make LaHIE available to Participants 24 hours a day, 7 days a week, excluding: (i) planned downtime for which Quality Forum has provided notice; or (ii) any unavailability caused by circumstances beyond Quality Forum's and/or Current Software Vendor's reasonable control including, without limitation, acts of God, strikes, lockouts, riots, acts of war, epidemics, governmental action after the date of this Agreement, fire, communication line failures, power failures, earthquakes, hurricanes or other disasters (collectively "Force Majeure"); however, LaHIE availability may be temporarily suspended for maintenance or unscheduled interruptions. Quality Forum will use its best efforts to provide reasonable advance notice, which will be no less than 24 hours advance notice, of any such known suspension or interruptions of LaHIE availability and to restore LaHIE availability as soon as reasonably possible. Participants who are Health Care Providers shall use reasonable efforts to obtain patient health information through other means during any periods when LaHIE is not available.

3.3 **Support Services.** During the Term of this Agreement and in consideration of the fees payable to Quality Forum as provided in Exhibit D-1, Quality Forum will provide limited support services to assist Participant in the implementation of the Technical Environment necessary to access LaHIE. Quality Forum will provide initial training to Participant through a train the trainer format on the access and use of LaHIE and will maintain a help desk that will provide telephone support regarding the use of LaHIE.

3.4 **LaHIE Records.** Quality Forum and/or Current Software Vendor will reasonably maintain certain records relating to the operation of LaHIE, including certain records of the date, time and records accessed by a Participant in each Data Exchange. Quality Forum will not maintain, and will not be responsible for maintaining, records of the content of any Data Exchange or for inspecting the content of Data.

3.5 **Policies and Procedures.** Quality Forum will establish a Policy Manual that consists of policies and procedures ("Policies and Procedures") that will govern Participants' activities on LaHIE, and these Policies and Procedures will be available on Quality Forum's website as they are implemented and/or revised. Quality Forum encourages Participant to provide input in the development of Policies and Procedures through Quality Forum's working groups and/or taskforces. These Policies and Procedures govern Participants' use of LaHIE and the use, submission, transfer, access, privacy and security of Data.

3.6 Changes to Policies and Procedures. Quality Forum may change or amend the Policies and Procedures from time to time at its discretion and will post notice of proposed and final changes on Quality Forum's website from time to time. Quality Forum will provide Participants notice of such changes to Policies and Procedures by electronic mail. Any changes will be effective 60 days following adoption by Quality Forum, unless Quality Forum determines that an earlier effective date is required to address a legal requirement, a concern relating to the privacy or security of Data or an emergency situation. Quality Forum also may postpone the effective date of a change if Quality Forum determines, in its sole discretion, that additional implementation time is required. Participant will have no ownership or other property rights in the Policies and Procedures or other materials or services provided by Quality Forum and/or the Current Software Vendor.

3.7 Security. Quality Forum will implement Policies and Procedures that are reasonable and appropriate to provide that Data Exchanges are authorized, to protect Data from improper access, tampering or unauthorized disclosure and to secure compliance with applicable laws and regulations. Such Policies and Procedures will include administrative procedures, physical security measures, and technical security services that are reasonably necessary to secure the Data. Participant will comply with the security Policies and Procedures established by Quality Forum, including the requirements set forth in Exhibit A.

3.8 Investigations, Corrections, Reports. Quality Forum will adopt Policies and Procedures for the investigation, resolution and reporting of Patient complaints, security breaches or other concerns relating to compliance with this Agreement, Quality Forum's Policies and Procedures and applicable laws and regulations ("Compliance Concerns"). Forum will provide notice to Participants, pursuant to Quality Forum's policy and as required by law or regulation, of any Compliance Concern related to Participant's Authorized Users' use of LaHIE, and Participant will cooperate with Quality Forum in its investigation of any Compliance Concern and corrective action.

3.9 Obligations to Comply with Law. Quality Forum will comply with all federal, state and local laws applicable to Quality Forum. This includes Title XIII, Subtitle D of the Health Information Technology for Economic and Clinical Health (HITECH) Act, codified at 42 U.S.C. §§ 17921-17954, and regulations issued by HHS to implement the HITECH Act, which are applicable to business associates, as of the date by which business associates are required to comply with such referenced statutes and HHS regulations.

3.10 Data Return. Quality Forum has no obligation to return to Participant any Data transferred or accessed pursuant to the terms of this Agreement.

3.11 Compliance With Business Associate Agreement. Quality Forum will fully comply with the terms of the Business Associate Agreement attached hereto as Exhibit C.

3.12 Special Provision for REC Eligible Hospitals. If Participant is a hospital that is also eligible (an "Eligible Participant") for Regional Extension Center Supplemental Grant Assistance through the Regional Extension Center Program (the "REC Program") administered by the Quality Forum, as determined by the Quality Forum in accordance with REC Program

guidelines, an Eligible Participant shall automatically be enrolled in the REC Program and entitled to receive the grant-subsidized benefits and services provided to hospital enrollees under the REC Program. In addition, all fees for the first two hundred (200) hours of technical assistance under the REC Program will be waived for any Eligible Participant.

#### 4. **SOFTWARE VENDOR ROLE**

4.1 Orion Selected As Current Software Vendor for LaHIE. Orion designs, manufactures and licenses software and provides services designed to manage clinical workflow and integration for the healthcare sector. Pursuant to a Software As A Service Agreement executed with Orion on August 3, 2011 (the “Software Vendor Agreement”), Quality Forum has chosen Orion as its Current Vendor Supplier and contracted for Orion to establish, implement and maintain LaHIE for use by Participants and Authorized Users who have executed a Participation Agreement with Quality Forum. Pursuant to the Software Vendor Agreement, Orion will implement the SaaS Service that forms the technological component of LaHIE and will host and maintain LaHIE on behalf of Quality Forum, which may replace the Current Software Vendor as Quality Forum deems necessary or appropriate. Participant acknowledges that: (i) Quality Forum is not a software developer; (ii) Quality Forum does not own and has not developed or implemented the technology that forms any component of the software or related technology associated with LaHIE; (iii) Quality Forum does not provide website hosting services and is not hosting LaHIE over the Internet; (iv) the Current Software Provider owns or otherwise controls the software and related technology associated with LaHIE; and (v) the Current Software Vendor has contracted to provide services and license the software and related technology associated with LaHIE to Quality Forum and to support and maintain LaHIE for and on behalf of Quality Forum.

4.2 Current Software Vendor’s Obligations To Maintain LAHIE. Pursuant to the Software Vendor Agreement, the Current Software Vendor has made extensive commitments to the Quality Forum regarding the reliable build-out and secure operation of LaHIE in compliance with applicable Federal and Louisiana laws, which commitments materially consist of following non-exclusive terms:

(a) Current Software Vendor will use all reasonable efforts to ensure that all transactions processed through LaHIE are backed up regularly and in accordance with agreed back up requirements and applicable industry standards. Current Software Vendor will maintain thirty days’ worth of verified backups.

(b) LaHIE and the use of the same by the Quality Forum and Participants shall not infringe the intellectual property rights of any person.

(c) All software and other technology provided by Current Software Vendor pursuant to the Software Vendor Agreement function in an integrated manner and will interface with third party software, including the software used by Participants in LaHIE, but only as agreed by the

parties pursuant to the Initial Statement of Work and/or in any subsequent SOWs executed by the parties.

(d) LaHIE as developed by Current Software Vendor (including the delivery of any upgrades and/or new versions) will not contain any viruses, Trojan horses, trap doors, back doors, Easter eggs, worms, time bombs, cancelbots, or other computer programming routines that are intended to damage, detrimentally interfere with, surreptitiously intercept, expropriate, or make any other unauthorized transfer, alteration or use of any information (“Viruses”).

(e) At Current Software Vendor’s expense as provided herein, Current Software Vendor agrees to defend, hold harmless and indemnify Quality Forum and Participants, including their respective directors, officers, agents, employees, and successors in interest from and against any claim, demand, suit or proceeding, arising out of any claim by a third party that Quality Forum’s and/or any Participant’s authorized use of LaHIE infringes a third party’s patent, copyright, trade secret or other intellectual property rights (collectively, “Claim(s)”), and shall indemnify Quality Forum and Participants for any damages finally awarded against them by a court or administrative body of competent jurisdiction, including without limitation, attorneys’ fees. Quality Forum and/or any involved Participants shall: (i) give Current Software Vendor reasonably prompt written notice of such Claim; and (ii) allow Current Software Vendor to control, and fully cooperate with Current Software Vendor (at the Current Software Vendor’s sole expense) in, the defense and all related negotiations.

(f) Current Software Vendor will not gather, store, log, archive, use or otherwise retain any Personal Data in any manner and will not disclose, distribute, sell, share, rent or otherwise transfer any Personal Data to any third party, except as expressly provided in the Software Vendor Agreement or as Software Vendor may be expressly directed in advance in writing by Quality Forum.

(g) Current Software Vendor shall ensure that its systems including specifically those systems associated with and/or hosting LaHIE include up-to-date anti-viral software to prevent viruses from reaching Quality Forum and/or Participants’ systems through Current Software Vendor’s systems. Current Software Vendor shall prevent unauthorized access to LaHIE systems through the Current Software Vendor’s systems.

(h) Current Software Vendor will make any modification or enhancement to LaHIE required to meet new federal or state legal requirements with respect to use or disclosure of PHI or participation in a HIE but only to the extent required for Customer to exchange information with the State of Louisiana, the Nationwide Health Information Network (“NHIN”) or NHIN Direct, relevant interstate HIEs, relevant medical home projects to the extent applicable, electronic health record vendors that offer data sharing services or technology; such modification(s) or enhancement(s) will be made free of charge to Quality Forum if made generally available and at no charge to Current Software Vendor’s customer base.

(i) Current Software Vendor has warranted that it will meet applicable standards and certification criteria pursuant to the American Recovery and Reinvestment Act, P.L. 111-05 (the “ARRA”), § 3004, as may be amended from time-to-time, for certification as a qualified

electronic health record (“EHR”) under § 3001(c)(5) of the ARRA and any such standard updates promulgated by regulations issued under the ARRA from time to time, but only to the extent Current Software Vendor is required by law to do so as a vendor supporting HIEs.

(j) If the State of Louisiana or the Certification Commission for Health Information Technology (“CCHIT”) requires an item of licensed Software to be certified by CCHIT or another nationally recognized certifying agency, Current Software Vendor has agreed to use commercially reasonable efforts to pursue such certification at no additional cost to Quality Forum.

(k) Current Software Vendor will take all reasonable commercial steps required to ensure that LaHIE is in compliance with HIE requirements imposed by federal laws or regulations and related health information technology requirements of the state of Louisiana.

(l) Current Software Vendor has agreed that it understands that Quality Forum is fully relying upon Current Software Vendor to ensure that LaHIE is and remains fully compliant with all state and federal applicable laws and regulations, including those now existing, later enacted and/or supplemented or revised.

(m) The ONC is defining criteria for clinicians to meet Meaningful Use (as defined in Subtitle D of the ARRA - the HITECH Act – and its enabling regulations) of EHRs. A subset of these criteria requires participation in a health information exchange. If future federal regulations require new software development to meet Meaningful Use criteria applicable to a health information exchange system, the programming cost of such development shall be the sole responsibility of Current Software Vendor.

(n) Current Software Vendor will use commercially reasonable best efforts to achieve certification requirements of the ONC on or before the compliance date including but not limited to compliance certification for the LaHIE (conditioned on Quality Forum and Participants providing reasonable cooperation requested by Current Software Vendor and that Quality Forum and all Participants complete their own responsibilities relating to HIE certification, if any, in a timely manner).

(o) Current Software Vendor has agreed to maintain a Disaster Recovery Plan for LaHIE and implement such plan in the event of any unplanned interruption of LaHIE. At a minimum, the Plan will meet or exceed industry standards and include redundant systems located in a separate State. Current Software Vendor shall actively test, review, and update the Plan on at least an annual basis.

## 5. **PARTICIPANT’S OBLIGATIONS**

5.1 Limitation of Use. Participant shall: (i) not access or use LaHIE except as provided herein and only for the Permitted Use specified in section 2.1; (ii) shall not let any other entity or person access or use LaHIE other than Participant’s Authorized Users; (iii) not attempt to gain, or assist others to gain unauthorized access to LaHIE and shall ensure that the access and use of LaHIE is properly restricted to its Authorized Users through the issuance and protection of

confidential passwords; (iv) promptly notify Quality Forum of any unauthorized access or unlicensed use of LaHIE; (v) use LaHIE only in accordance with applicable federal and state laws, and government regulations, including federal and state laws pertaining to privacy and security of Data; (vi) not interfere or disrupt the integrity or performance of LaHIE or any Data contained therein; (vii) ensure that access and use of LaHIE is limited to Authorized Users that have been trained to use LaHIE and are able to competently do so in accordance with this Agreement and any supporting documentation that is provided and/or made available to Participant; (viii) not alter or modify Current Software Vendor's underlying software and/or technology associated with LaHIE; (ix) timely pay to Quality Forum the fees specified in Schedule D; (x) act to ensure that any Data entered into LaHIE by Participant and/or on its behalf is accurately entered and materially complete; and (xi) fully comply with the terms of this Agreement and the Policies and Procedures referenced in subsection 3.6, which, as amended and revised from time to time, are fully adopted and incorporated into this Agreement as if expressly written herein.

5.2 Technical Environment Requirements. Participant will be responsible for ensuring that it meets the Technical Environment in all material respects as set forth in Exhibit E. Participant shall be solely responsible for any corresponding failure and/or reduction in Participant's ability to access and/or use LaHIE where the Participant has not met or maintained the Technical Environment in all material respects and the failure directly results therefrom. Participant will ensure that any Data it provides or submits can be related to and identified with source records maintained by Participant and will make any such Data available for LaHIE in accordance with the scope, format and specifications set forth.

5.3 Security Protocols. Participant acknowledges that LaHIE will be accessed using unique user identifications and passwords, and agrees that Participant has sole responsibility for the creation of such unique identifiers and reasonably maintaining the confidentiality and security of the passwords used to access LaHIE. In accordance with this Agreement and Quality Forum's Policies and Procedures, Participant will identify and authenticate its Authorized Users who may use LaHIE for the Permitted Use on behalf of Participant and will require each Authorized User to execute an Authorized User Agreement in the form of the agreement attached hereto as Exhibit B. Participant is and shall remain solely responsible for its Authorized Users' compliance with the terms and conditions of this Agreement, the Policies and Procedures, the Authorized User Agreement and applicable laws and regulations. Quality Forum shall have no liability to Participant or any third party whatsoever for any unauthorized access to LaHIE or any Data resulting from a failure of Participant and/or its Authorized Users to reasonably maintain the confidentiality and security of its passwords. Participant agrees that it will install and maintain appropriate and commercially reasonable security solutions to deter unauthorized access to its network and LaHIE, including adequate firewall, intrusion detection, anti-virus and security solutions.

5.4 Reliance Upon Participant. Participant acknowledges that Forum and the Current Software Vendor will rely upon the reasonable accuracy and completeness of technical information and materials provided by Participant and relating to Participant's technological systems, components and/or Data, and agrees that all such information disclosed to Forum and/or the Current Software Vendor is derived from Participant's qualified personnel in the areas

required, and is true, accurate and not misleading in any material respect (or will be at the time of disclosure).

5.5 Patient Consents. The parties acknowledge that certain uses of Data, including, without limitation Treatment, Payment and certain Health Care Operations (as defined by the HIPAA Standards for Privacy of Individually Identifiable Health Information, 45 C.P.R. Part 164, Subpart E) does not require specific consent by a Patient under HIPAA or Louisiana Law for these purposes. Participant will fully comply with the terms of the Business Associate Agreement attached hereto as Exhibit C.

5.6 Authorized Users. In accordance with this Agreement and Quality Forum's Policies and Procedures, Participant will identify and authenticate its Authorized Users who may use LaHIE for the Permitted Use on behalf of Participant and will require each Authorized User to execute an Authorized User Agreement that is substantially equivalent to the form of the agreement attached hereto as Exhibit B. Participant is responsible for Authorized Users' compliance with the terms and conditions of this Agreement and applicable laws and regulations.

5.7 System Operations. Participant, at its own expense, will provide and maintain the equipment, software, services and testing necessary to effectively and reliably participate in LaHIE as set forth in Exhibit C, except for such software expressly provided by Quality Forum and/or Current Software Vendor pursuant to Section 4.

5.8 Record Retention, Storage and Backup. Participant, at its own expense, will perform Data backup and retention to maintain adequate records of any Data submitted to LaHIE. If Participant is a Health Care Provider, it will maintain at its own expense records of Data accessed through LaHIE and used by Health Care Provider for Patient Treatment. Said Participant will maintain these records for all periods required by law and is solely responsible for determining the form for such records, which may include incorporation of Data into the Health Care Participant's medical records electronically, by hard copy or by other form of summary, notation or documentation.

5.9 Data Accuracy. Participant is solely responsible for the accuracy of any Data submitted to LaHIE by Participant and/or on its behalf. Participant will promptly correct any errors discovered in Data it transmits to LaHIE and will notify Quality Forum in writing of any such corrections pursuant to Quality Forum's Policies and Procedures.

5.10 Testing Obligations. Participant acknowledges and agrees they comply with all timetables and schedules provided by Quality Forum and/or Current Software Vendor regarding implementation of Technical Environment and testing of Participant's test data. Participant agrees to make its test data and Technical Environment available for testing and implementing LaHIE for timely access and use by said Participant and/or its Authorized User.

5.11 Prompt Responses and Cooperation. Participant shall reasonably cooperate with Quality Forum and/or Current Software Vendor's personnel in respect of any reasonable request made by Quality Forum and/or Current Software Vendor for the purposes of Current Software Vendor satisfying any implementation, testing and/or any go-live dates established by the parties.

Participant understands and agrees that its participation and timely responsiveness is required in order for Current Software Vendor to timely implement LaHIE for Participant's access and use and Participant therefore agrees to promptly respond to requests from Quality Forum and Current Software Vendor and to provide data, technical information and/or documentation, as requested. Participant further agrees to ensure that its technical personnel involved in Participant's migration to LaHIE are suitably qualified with sufficient skills and expertise in the software applications and business practices used by Participant to carry out Participant's responsibilities under this Section 5.

5.12 Failure to Timely Cooperate. Participant agrees that its priority status for incorporation into and/or access of LaHIE is entirely dependent upon its timely compliance with this Section 5 and related applicable provisions of this Agreement.

5.13 Compliance with Laws. Participant agrees to comply with HIPAA and HITECH (as those terms are defined in the Agreement) and Louisiana state law with respect to any use or disclosure by Participant of Data in connection with their participation in LaHIE.

5.14 Indemnity. Participant will indemnify Quality Forum, Orion and/or the Current Software Vendor for any breach of the Participant's obligations under this Agreement.

5.15 Sole Liability for Data Input. Participant will be solely responsible for the accuracy, quality, integrity, and legality of any Data input into LaHIE by Participant.

5.16 Trained Personnel. Participant agrees to ensure that use of LaHIE and underlying software and technology is performed in accordance with any provided documentation and this Agreement and only by trained employees or persons under their supervision.

5.17 Satisfaction of Technical Environment. Participant agrees to ensure that its computer systems and any other specified technology required to use LaHIE will meet the Technical Environment Specifications.

## 6. **CONFIDENTIALITY.**

In addition to each party's obligation to comply with federal and state laws relating to protection and security of the Data, Quality Forum and Participant, including their respective agents and employees, will treat any Data involving the identity of any patient as confidential information and will maintain the confidentiality of such identifying information, subject to disclosure and use only through LaHIE as provided herein.

## 7. **FEES AND PAYMENT**

7.1 Payment of Fees. Participant will timely pay Quality Forum the fees set forth in Exhibit D and Exhibit D-1.

7.2 Interest. Any fees that are not timely paid by Participant as provided herein shall accrue interest as specified in Exhibit D from the due date until paid.

7.3 Annual Fees. Any fees chargeable to Participant annually shall be eligible for annual fee increases, which shall be limited to (i) the greater of the CPI or (ii) Three and one half percent (3.5%) per year over the prior year's fee. To the extent reasonable possible, Forum shall advise Participant in writing of any annual fees increases within 60 days of the applicable anniversary date of the Effective Date.

## 8. PROPRIETARY INFORMATION

During the Term of this Agreement, each party may have access to information about the other party that: (a) relates to past, present or future business activities, practices, protocols, products, services, information, content, and technical knowledge; and (b) has been identified as confidential (collectively, "Proprietary Information") by such party. For the purposes of this provision, Proprietary Information will not include Data.

8.1 Non-disclosure. The parties will: (a) hold Proprietary Information in strict confidence; (b) not make the Proprietary Information available for any purpose other than as specified in the Agreement or as required by law or subpoena; and (c) take reasonable steps to ensure that the Proprietary Information is not disclosed or distributed by employees, agents or consultants (who will have access to the same only on a "need-to-know basis") to third parties in violation of this Agreement. If Quality Forum or Participant receives a request for Proprietary Information, the party receiving the request will provide the other party notice of the request and an opportunity to seek a protective order limiting the nature and scope of the information to be disclosed, and the disclosing party is only permitted to disclose Proprietary Information to the extent required by law.

8.2 Exclusions. Proprietary Information will not include information that: (a) at the time of disclosure, is known or becomes known or available to general public through no act or omission of the receiving party; (b) was in the receiving party's lawful possession before it was provided to the receiving party by the disclosing party; (c) is disclosed to the receiving party by a third party having the right to make such disclosure; or (d) is independently developed by the receiving party without reference to the disclosing party's Proprietary Information. Unless one or more of these exclusions is demonstrated prior to disclosure, the parties will apply a presumption that information is Proprietary Information.

8.3. Equitable Remedies. The parties agree that a breach of this Section will cause the disclosing party substantial and continuing damage, the value of which will be difficult or impossible to ascertain, and other irreparable harm for which the payment of damages alone will be inadequate. Therefore, in addition to any other remedy that the disclosing party may have under this Agreement, at law or in equity, in the event of such a breach or threatened breach by the receiving party of the terms of this Section, the disclosing or non-breaching party will be entitled, after notifying the receiving, or breaching, party in writing of the breach or threatened breach, to seek both temporary and permanent injunctive relief without the need to prove damage, irreparable injury or post bond.

## 9. **ELECTRONIC SIGNATURES**

9.1 **Signatures and Signed Documents.** Participant, at Quality Forum's request, will implement for its Authorized Users an electronic identification consisting of symbols or codes that are to be affixed to or contained in a Data Exchange made by the Participant ("Signatures"). Participant agrees that any Signature of such party affixed to or contained in any Data Exchange will be sufficient to verify that the party originated such Data Exchange. Any properly transmitted Data Exchange made pursuant to this "writing" or "in writing" and any such Data Exchange when containing, or to which there is affixed, a Signature ("Signed Documents") shall be deemed for all purposes: (a) to have been "signed;" and (b) to constitute an original when printed from electronic files or records established and maintained in the normal course of business.

9.2 **Validity of Signed Documents.** Participant will not contest the validity or enforceability of Signed Documents under the provisions of any applicable law relating to whether certain agreements are to be in writing or signed by the party to be bound thereby. Signed Documents, if introduced as evidence on paper in any judicial, arbitration, mediation, or administrative proceedings, will be admissible as between the parties to the same extent and under the same condition as other business records originated and maintained in paper form.

## 10. **TERM AND TERMINATION**

10.1 **Term and Termination.** The Term of this Agreement will begin on the Effective Date and will continue thereafter for a period of five (5) years unless terminated as set forth in this Section 10. This Agreement will terminate under any of the following circumstances:

10.1.1 **Violation of Law or Regulation.** If either Quality Forum or Participant reasonably determines that its continued participation in this Agreement would cause it to violate any law or regulation applicable to it, or would place it at material risk of suffering any sanction, penalty, or liability, then that party may terminate its participation in this Agreement immediately upon written notice to the other party.

10.1.2 **For Cause.** If Quality Forum or Participant determines that the other party or any of its employees, agents or contractors have materially breached this Agreement, then that party may terminate its participation in this Agreement on 30 days' advance written notice to the other party, provided that such notice identifies such area of non-compliance, and such non-compliance is not cured within 30 days of receipt of the notice of non-compliance. Quality Forum may immediately terminate this Agreement upon written notice to Participant if Forum determines that Participant or its Authorized Users, employees or agents have accessed or used Data or LaHIE for any purpose other than the Permitted Use or in violation of security or privacy provisions under this Agreement or applicable laws and regulations.

10.1.3 **Insufficient Participation.** Quality Forum and Participant acknowledge and agree that by entering into this Agreement they intend to promote the electronic sharing of healthcare information across computerized networks and amongst multiple

health care providers. If after three (3) years from the Effective Date there is insufficient participation in LaHIE by other Participants to reasonably justify Participant's continued participation in LaHIE (a "Deficiency"), Participant may give Quality Forum ninety (90) days advance written notice of Participant's intent to terminate this Agreement. Such written notice shall include an explanation of the basis upon which Participant alleges that termination of the Agreement for the Deficiency is justified. If Quality Forum does not agree that termination under this Section 10.1.3 is reasonably justified, the parties shall negotiate in good faith for a period not to exceed the ninety (90) day notice period in an effort to resolve the dispute. If the parties are unable to resolve the dispute during such ninety (90) day period, either party may immediately terminate this Agreement and pursue its legal remedies. If Quality Forum agrees that termination under this Section 10.1.3 is otherwise reasonably justified, Quality Forum shall have the ninety (90) day notice period to cure the Deficiency. If after ninety (90) days the parties disagree as to whether the alleged Deficiency has been cured, either party may immediately terminate this Agreement and pursue its legal remedies.

10.2 Termination Process and Access to LaHIE and Data. Upon the effective date of any termination or expiration of this Agreement, Quality Forum will cease providing access to LaHIE for the Participant and its Authorized Users, and Participant and its Authorized Users will stop accessing, attempting to access, and/or using LaHIE.

### 10.3 Effect of Termination.

10.3.1 Rights and Duties. Any termination will not alter the rights or duties of the parties with respect to Signed Documents transmitted before the effective date of the termination or with respect to fees outstanding and payable under this Agreement. The provisions of this Agreement which should by their nature survive termination or expiration, shall survive termination or expiration of this Agreement.

10.3.2 Return of Proprietary Information; Software; Fees. Within 30 days of the effective date of termination or expiration, each party will return to the other all Proprietary Information belonging to the other or certify the destruction of such Proprietary Information if agreed to by the party who originated the Proprietary Information. Within 30 days of the effective date of termination, Participant will un-install and return to Quality Forum all software provided by Quality Forum to Participant under this Agreement. If Participant has prepaid any fees as of the effective date of termination, Participant will be entitled to a pro rata refund of such advance payment if the Agreement has been properly terminated for cause by Participant. Otherwise, no refunds of any nature will be due. No Data will be returned to a Participant upon termination of this Agreement.

## 11. **LIMITED WARRANTY AND DISCLAIMER OF OTHER WARRANTIES**

Limited Warranty and Disclaimer of Other Warranties. Participant acknowledges and agrees that Quality Forum is neither a manufacturer, developer, reseller and/or owner of the SaaS Service or any other technology associated with LaHIE. As such, Quality Forum only agrees to

comply with the terms of this Agreement and to use its commercially reasonable best efforts to maintain the satisfactory operation of LaHIE, as provided herein. **QUALITY FORUM MAKES NO REPRESENTATION OR WARRANTY THAT ANY DATA WILL BE ACCURATE, TIMELY, OR COMPLETE. QUALITY FORUM MAKES NO WARRANTY OR REPRESENTATION REGARDING THE ACCURACY OR RELIABILITY OF ANY INFORMATION TECHNOLOGY SYSTEM USED FOR LAHIE. QUALITY FORUM DISCLAIMS ALL WARRANTIES REGARDING ANY PRODUCT, SERVICES, OR RESOURCES PROVIDED BY IT, OR DATA EXCHANGES TRANSMITTED PURSUANT TO THIS AGREEMENT, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, TITLE, OR NON-INFRINGEMENT. QUALITY FORUM PROVIDES NO OTHER EXPRESS OR IMPLIED WARRANTIES. THESE DISCLAIMERS WILL APPLY UNLESS APPLICABLE LAW DOES NOT PERMIT THEM.**

## 12. **LIMITATION OF LIABILITY; INDEMNIFICATION**

12.1 **Limitation of Liability.** Neither Quality Forum nor Participant will be liable to the other for lost profits or Data, or any special, incidental, exemplary, indirect, consequential or punitive damages (including loss of use or lost profits) arising from any delay, omission or error in a Data Exchange or receipt of Data, or arising out of or in connection with this Agreement, whether such liability arises from any claim based upon contract, warranty, tort (including negligence), product liability or otherwise, and whether or not either party has been advised of the possibility of such loss or damage.

12.2 **Release of Liability.** Participant releases Quality Forum from any claim arising out of any inaccuracy or incompleteness of Data or any delay in the delivery of Data or failure to deliver a Data Exchange when requested except for those arising out of Quality Forum's gross negligence.

### 12.3 **Indemnification.**

12.3.1 **Indemnification for Infringement.** Quality Forum and/or Current Software Vendor will indemnify and hold harmless Participant, its employees and agents from any damages, expenses and costs, including reasonable attorneys fees, arising out of claims by third parties that the use of LaHIE and any Software provided by the Current Software Vendor infringes any patents, copyrights or trademarks, provided that Participant notifies Quality Forum in writing promptly upon discovery of any such claim and gives Quality Forum and/or the Current Software Vendor complete authority and control of, and full cooperation with, the defense and settlement of such claim.

12.3.2 **Indemnification for Breach of Agreement.** Participant will indemnify and hold harmless Quality Forum, its employees and agents from any damages, expenses and costs, including reasonable attorneys fees, from claims by third parties arising from Participant's, or its Authorized Users', breach of this Agreement or the Authorized Users Agreement, including the unauthorized or improper access or use of LaHIE or

Participant's or its Authorized Users' use or disclosure of Data for any purpose other than a Permitted Use. Quality Forum will indemnify and hold harmless Participant, its employees and agents from any damages, expenses and costs, including reasonable attorneys' fees, from claims by third parties arising from Quality Forum's breach of this Agreement, including the unauthorized or improper use of LaHIE or Quality Forum's unlawful use or unlawful disclosure of Data.

12.4 Indemnity Amongst Participants. Participant (as the "Indemnifying Participant") agrees to defend, indemnify and hold harmless the Quality Forum and any other Participant that is named a defendant in any litigation or proceeding by any Patient or family member of any Patient as a result of any breach of this Agreement by the Indemnifying Participant and/or its Authorized Users, including without limitation any unauthorized access of Data or any access of Data for any improper purpose such as "curiosity viewing." To the extent the Indemnifying Participant fails or refuses to defend and/or indemnify the Quality Forum and/or any other named Participant as required herein, the Indemnifying Participant hereby agrees that the Quality Forum and/or the named Participant may add the Indemnifying Participant as a third party defendant or co-defendant to any such litigation or proceeding and legally assert its claims for indemnification hereunder.

12.5 Not a Medical Service. **LaHIE does not make clinical, medical or other decisions and is not a substitute for professional medical judgment applied by Participant or its Authorized Users. Participant and its Authorized Users are solely responsible for confirming the accuracy of all Data and independently making all medical and diagnostic decisions.**

### 13. OWNERSHIP AND INTELLECTUAL PROPERTY

13.1. Current Software Vendor Technology. Participant acknowledges and agrees that Current Software Vendor has reserved and retained for itself and/or its licensors all rights, title and interest in and to the SaaS Service and underlying technology. Except for the license rights expressly granted in this Agreement, no express or implied license, right or interest in or to any intellectual property of Current Software Vendor or its licensors is conferred by this Agreement.

13.2 Ownership of Data. Participant acknowledges and agrees that Data entered into LaHIE will be aggregated with other Data and that Quality Forum is and shall remain the sole and exclusive owner of any and all Data entered into LaHIE, both aggregated and non-aggregated. Notwithstanding the foregoing, Participant will retain whatever proprietary rights it may possess in and to any separate data that remains in Participant's own database of records.

### 14. GENERAL PROVISIONS

14.1 No Exclusion. Quality Forum represents and warrants to Participant, and Participant represents and warrants to Quality Forum, that neither party nor their respective employees or agents have been placed on the sanctions list issued by the Office of the Inspector

General of the Department of Health and Human Services pursuant to the provisions of 42 U.S.C. 1320a(7), have been excluded from government contracts by the General Services Administration or have been convicted of a felony or any crime relating to health care. Quality Forum and Participant will provide one another immediate written notice of any such placement on the sanctions list, exclusion or conviction.

14.2 Severability. Any provision of this Agreement that is determined to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this Agreement or affecting the validity or enforceability of such remaining provisions.

14.3 Entire Agreement. This Agreement constitutes the complete agreement of the parties relating to the matters specified in this Agreement and supersedes all earlier representations or agreements with respect to the subject matter of this Agreement, whether oral or written with respect to such matters. No oral modification or waiver of any of the provisions of this Agreement is binding on either party.

14.4 No Assignment. Neither Quality Forum nor Participant may assign its rights or obligations under this Agreement without the advance written consent of the other party, except for a transfer or assignment to a parent, subsidiary or affiliate wholly owned by the party.

14.5 Governing Laws. This Agreement is governed by and interpreted in accordance with Louisiana laws, without regard to its conflict of law provisions. The parties agree that exclusive jurisdiction over any action arising out of or relating to this Agreement shall be in the State of Louisiana and all claims arising hereunder shall be exclusively resolved through the courts existing in East Baton Rouge Parish and all parties hereto submit themselves to the jurisdiction of the courts in East Baton Rouge Parish for all claims arising hereunder.

14.6 Force Majeure. No party is liable for any failure to perform its obligations under this Agreement, where such failure results from any act of God or other cause beyond such party's reasonable control (including, without limitation, any mechanical, electronic, or communications failure).

14.7 Notices. All notices, requests, demands, and other communications required or permitted under this Agreement will be in writing. A notice, request, demand, or other communication will be deemed to have been duly given, made and received: (a) when personally delivered; (b) on the day specified for delivery when deposited with a courier service such as Federal Express for delivery to the intended addressee; or (c) three business days following the day when deposited in the United States mail, registered or certified mail, postage prepaid, return receipt requested, addressed as set forth on the page one of this Agreement with regard to Participant and addressed as follows with regard to Quality Forum:

Louisiana Health Care Quality Forum  
Attn: Executive Director  
8550 United Plaza Blvd., Suite 500  
Baton Rouge, LA 70809

Nothing in this section will prevent the parties from communicating via electronic mail, telephone, facsimile, or other forms of communication for the routine administration of LaHIE.

14.8 No Agency. Quality Forum provides LaHIE services to Participant but does not act as Participant's agent. Participant will not be deemed an agent of another Participant as a result of participation in this Agreement. Participant acknowledges and agrees that the Current Software Vendor is not an agent or representative of the Quality Forum and Quality Forum shall have no liability for any acts or omissions of the Current Software Vendor.

14.9 No Relationship between Participants; No Third Party Rights. Nothing in this Agreement confers any rights or remedies under this Agreement on any persons other than Quality Forum and Participant, and nothing in this Agreement is intended to create a contractual relationship or otherwise affect the rights and obligations among Participants. Nothing in this Agreement will give any third party, including other Participants, any right of subrogation or action against any party to this Agreement.

**SIGNED** on behalf of **Participant**: by:

Signature:	_____	Witness:	_____
Name/Title:	_____	Name:	_____
Date:	_____	Address:	_____
		Occupation:	_____

**SIGNED** on behalf of **LOUISIANA HEALTH CARE QUALITY FORUM** by:

Signature:	_____	Witness:	_____
Name/Title:	_____	Name:	_____
Date:	_____	Address:	_____
		Occupation:	_____

## EXHIBIT A

### PARTICIPANT SECURITY REQUIREMENTS

In addition to any obligations set forth in the Agreement and Quality Forum's Policies and Procedures, Participant will observe the following requirements. Quality Forum may amend or supplement these requirements on written notice to Participant.

1. Each of Participant's servers connecting to the LaHIE gateway will comply with Quality Forum's authentication requirements, implementing Secure Sockets Layer (SSL) encryption and using certificates approved by Quality Forum.
2. Participant will authenticate each Authorized User at the point of access and will implement password policies, both based on applicable laws and regulations and Quality Forum's Policies and Procedures. Participant may elect to implement stronger authentication mechanisms at its discretion. Participant will review and update its list of Authorized Users as required under Quality Forum's Policies and Procedures.
3. Participant will limit access of each Authorized User to a Permitted Use and according to Role Based Access principles. Participant will impose appropriate sanctions for its employees or agents who violate applicable security Policies and Procedures or the Authorized User Agreement or make improper use of LaHIE or its associated Data, including revocation of an Authorized User's authorization to access LaHIE as may be appropriate under the circumstances. In the event of any such violation, Participant will promptly notify Quality Forum in writing and fully describe said violation.
4. Participant will maintain access logs that capture Authorized User identification information.
5. Each of the Participant's servers exchanging Data with the LaHIE interface gateway will use an industry standard encryption method, such as IP-SEC.
6. Participant will implement firewalls and intrusion detection per Quality Forum's Policies and Procedures.
7. Participant will implement other safeguards to protect servers based on information security best practices, such as the SANS Institute ([www.sans.org](http://www.sans.org)) recommendations.
8. Participant will perform periodic automated and random manual review and verification of audit logs for both operational monitoring and system security as required by Quality Forum's Policies and Procedures.

## **EXHIBIT B**

### **SAMPLE AUTHORIZED USER AGREEMENT**

The Louisiana Health Information Exchange (“Exchange”) facilitates the electronic availability of protected health information (“Data”) through LaHIE to individuals and organizations that have contracted with the Louisiana Health Care Quality Forum (“Forum”) in order to assist Health Care Providers in providing treatment to Patients. Participant (defined below) has entered into a Participation Agreement with Forum in order to facilitate this exchange of Data for these purposes.

You have been identified by Participant as an Authorized User of Data that may be shared through LaHIE. Forum will agree to provide access to LaHIE and its Data to you through LaHIE, only if you agree to the terms and conditions of this Agreement.

1. Compliance with Agreement. THIS IS A BINDING AGREEMENT. By signing below, you agree to comply with all terms and conditions of this Agreement for access to and use of LaHIE and any Data shared through LaHIE, as authorized by the Participant's Participation Agreement and Forum's Policies and Standards. Failure to comply with these terms and conditions may be grounds for discipline, including without limitation, denial of your privileges to access LaHIE and termination of your employment or agency by Participant.

2. Permitted Use and Restrictions on Use.

a. Participant is a Health Care Provider who provides Treatment to Patients, as defined by the HIPAA Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subpart E. As Participant's Authorized User, you may access LaHIE only to obtain Data to provide Treatment for Participant's Patients and/or for such other purposes as are permitted under section 3.1 of the Participation Agreement. You may not access or use LaHIE, or any hardware or software relating to use of LaHIE, for any purposes that are outside the scope of your duties with Participant to provide Treatment to Patients.

b. This Consent grants you a nonexclusive, nontransferable right to access and use LaHIE as provided herein and in the Participation Agreement. This right is subject to the following restrictions:

i. This right is specific to you. You may not share, sell, assign or sublicense this right with anyone else.

ii. You may not change, reverse engineer, disassemble or otherwise try to learn the source code, structure or ideas underlying LaHIE's software or introduce a virus to LaHIE. You may not connect or install unauthorized or uncertified equipment, hardware or software or improperly use the hardware or software relating to use of LaHIE.

3. Protection of Data.

a. Conditions of Access. As an Authorized User, you may have access to Data that includes protected health information that is subject to confidentiality, privacy and security requirements under state and federal law and regulations and/or the Participation Agreement. You agree that you will only access Data consistent with your access privileges, and pursuant to all requirements under this Agreement, the Participant's Participation Agreement, Forum Policies and Standards, and applicable laws and regulations.

b. Protection of Data. As an Authorized User, you have an obligation to maintain the confidentiality, privacy and security of the Data.

i. You will not disclose Data except as required for your job with Participant and subject to all terms of this Agreement and the Participation Agreement..

ii. You will not access or view any information other than what is required for you to do your job.

iii. You will not make any unauthorized copies of Data. You will not save Confidential Information to portable media devices (e.g., laptop computers, floppies, ZIP disks, CDs, PDAs, and other devices).

iv. You will not to email any Data to another email account.

v. You will not release your authentication code or device or password to any other person, including any employee or person acting on your behalf. You will not allow anyone else to access LaHIE under your authentication code or device or password. You agree not to use or release anyone else's authentication code or device or password. You agree to notify Forum and Participant immediately if you become aware or suspect that another person has access to your authentication code or device or password.

vi. You agree not to allow your family, friends or other persons to see the Data on your computer screen while you are accessing LaHIE. You agree to log out of LaHIE before leaving your workstation to prevent others from accessing LaHIE.

vii. You agree never to access Data for "curiosity viewing." This includes viewing Data of your children, other family members, friends, coworkers, or other persons of interest unless access is necessary to provide services to a Patient with whom you or the physician(s) with whom you work have a treatment relationship with that Patient.

viii. You will protect the accuracy of the Data submitted or received through LaHIE and will not insert information that you know is not accurate.

4. Audit and Review. Forum and Participant have the right at all times and without notice to access LaHIE and any hardware or software relating to LaHIE to review and audit your use of

LaHIE and compliance with the terms of this Agreement. This includes any hardware or software located at your office, your home, or any other site from which you access LaHIE.

5. Sanctions. You understand that failure to comply with the terms of this Agreement may result in disciplinary action against you, which may include loss of access to LaHIE as an Authorized User or termination of your employment or contract with Participant.

6. Duration. This Agreement will be in effect from the time it is signed until Forum or Participant terminates your status as an Authorized User or until you violate the terms of this Agreement. Any terms of this Agreement necessary to protect LaHIE and Data will survive the termination of this Agreement.

Agreed to by:

\_\_\_\_\_  
Authorized User Signature

\_\_\_\_\_  
Authorized User Printed Name

\_\_\_\_\_  
Date

\_\_\_\_\_  
Participant:

## **EXHIBIT C**

### **BUSINESS ASSOCIATE AGREEMENT**

On this \_\_\_ day of \_\_\_\_\_, 20\_\_, the undersigned, \_\_\_\_\_, (“Participant”), and Louisiana Health Care Quality Forum, a Louisiana non-profit corporation doing business as LaHIE (“Forum”), enter into this Business Associate Agreement (Agreement).

**WHEREAS**, Participant is either a “covered entity” within the meaning of 45 CFR 160.102, the “business associate” within the meaning of 45 CFR 160.102, or the subcontractor of a business associate; and

**WHEREAS**, either as a business associate or a subcontractor, Forum is required to comply with the HIPAA Privacy and Security Standards (45 CFR Parts 160 and 164) and the Health Information Technology for Economic and Clinical Health Act (“HITECH”), (collectively, the “Rule”); and

**WHEREAS**, Forum is specifically subject to 45 CFR Sections 164.308, 164.310, 164.312, 164.316 and 164.504(e); and

**WHEREAS**, Participant and Forum have entered into a contract (“Contract”) under which Forum provides, for or on behalf of Participant, certain products and/or services (“Covered Services”) and, in the process, uses, discloses, creates or receives individually identifiable health information which is protected under the Rule (“protected health information” or “PHI”).

**THEREFORE**, as a result, Participant and Forum enter into this Agreement in order to comply with the Rule.

**1. Uses and Disclosures of PHI:**

(A) Except as provided in Paragraph 2, Forum is permitted and/or required to use and disclose the PHI it obtains pursuant to the Contract and/or in the process of furnishing the Covered Services, only as described in the Contract or this Agreement (“Permitted Uses and Disclosures”). Forum is prohibited from any use or disclosure beyond the Permitted Uses and Disclosures without written permission of Participant. Forum is specifically prohibited from any use or disclosure of the PHI that would violate the requirements of the Rule, if done by the Participant.

(B) Forum shall comply with any obligations and restrictions on the use, disclosure or request for PHI contained Participant’s Notice of Privacy Practices required by 45 CFR §164.520, provided that Participant complies with Section 4(D) of this Agreement

2. **Other Permitted Uses and Disclosures:** Notwithstanding Paragraph 1, Forum may use the PHI:

(A) To perform data aggregation services (as permitted by 45 CFR § 164.504(e)(2)(i)(B)), the creation of a limited data set (as described in and limited by 45 CFR § 164.514(e)), or the de-identification of PHI as provided in 45 CFR 164.514, if not prohibited by the Contract;

(B) To report violations of law to appropriate Federal and State authorities, consistent with 45 CFR § 164.502(j)(1);

(C) For a use that is necessary for the proper management and administration of Forum or to carry out its legal responsibilities; and

(D) For a disclosure that is necessary for the proper management and administration of the Forum or to carry out its legal responsibilities, but only if:

(1) The disclosure is required by law; or

(2) Forum obtains reasonable assurances from the person to whom the PHI is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies Forum of any instances of which it is aware in which the confidentiality of the PHI has been breached.

3. **Other Obligations of Forum:** In addition to the foregoing, Forum shall, with regard to the PHI:

(A) Not use or further disclose the PHI other than as permitted or required by the Contract (as modified by this Agreement), by the individual as permitted or required by the Rule, or as required by law;

(B) Implement administrative, physical, and technical safeguards that prevent use or disclosure of the information other than as provided for by the Contract (as modified by this Agreement) and reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of Participant

(C) Promptly, but not in any case later than thirty days from discovery, report to Participant any security incident of which it becomes aware and any other use or disclosure of the information not provided for by the Contract (as modified by this Agreement) of which it becomes aware, have in place procedures to mitigate any harmful effects from the inappropriate use or disclosure, and mitigate, to the extent practicable, any harmful effect that is known to Forum of a use or disclosure of Protected Health Information by Forum in violation of this Agreement. Further, to the extent that such

unauthorized use or disclosure constitutes a breach within the meaning of the 42 USC 17921(1) or the Rule:

(1) Forum shall notify Participant of the breach without unreasonable delay but in no case later than 30 calendar days after the first day on which such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the Forum.

(2) The notification to Participant shall include, to the extent possible, (1) the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the Forum to have been, accessed, acquired, used, or disclosed during the breach; (2) a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (3) a description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved); (4) any steps individuals should take to protect themselves from potential harm resulting from the breach; and (5) a brief description of what the Forum is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches.

(D) Ensure that any agents, including a subcontractor, to whom it provides the PHI agrees in writing to the same obligations, terms, restrictions and conditions that apply to Forum under this Agreement. This provision shall not, however, be deemed to provide Forum with a right to assign or subcontract its responsibilities, except as specifically provided in the Contract.

(E) In the event of a request by the individual pursuant to the Rule (45 CFR §164.524 and 42 USC 17935(e)) for access to PHI, to the extent that said PHI is a designated record set in the possession of Forum, at the option of Participant either promptly make the PHI available directly to the individual or make the PHI available to Participant for the purpose of providing access to the individual. If the PHI requested is part of Participant's electronic health record, upon request of the individual the copy will be provided in an electronic format and, if the individual chooses, it will be directed to an entity or person designated by the individual, provided that said request is clear, conspicuous, and specific. Charges made by Forum for such access shall be limited to the amount provided in the Rule;

(F) In the event of a request by the individual pursuant to the Rule (45 CFR §164.526) to amend PHI to the extent that said PHI is a designated record set in the possession of Forum, either promptly comply with the applicable provisions of the Rule or make the PHI available to Participant for amendment. In the event that Participant accepts the amendment, incorporate said amendments to the PHI maintained by Forum as required by the Rule;

(G) To the extent required by the Rule or other applicable law, maintain data on all disclosures of PHI for which accounting is required by 45 CFR 164.528 for at least six years after the date of such disclosure, provided however that the obligation to maintain data on disclosures of PHI from electronic health records for treatment, payment and healthcare operations (“EHR Disclosures”) shall be maintained for three years. In the event of a request for an accounting of disclosures pursuant to the Rule (45 CFR §164.528 and 42 USC 17935(c)), at the option of Participant, Forum will either provide the disclosure as required therein or make that data available to Participant according to CE’s current written policy;

(H) Make its internal practices, books, and records relating to the use and disclosure of the PHI available to the Secretary for purposes of determining the Participant’s compliance with the Rule;

(I) At termination of the contract, to the extent feasible, recover all PHI in the possession of its agents and subcontractors and return or destroy all of the PHI that Forum still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the Contract (as modified by this Agreement) to the remaining PHI and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

(J) Not receive anything of value in exchange for the use or disclosure of protected health information except as permitted by 42 USC 17935(d), the Rule, and Participant.

(K) Not receive anything of value in exchange for communication about a product or service that encourages the recipients of the communication to purchase or use the product or service when such communication is prohibited by 42 USC 17935(d), the Rule, other applicable regulations, or this Agreement.

(L) Use and disclose only the minimum amount of protected health information necessary for the task at hand. To the extent possible, such minimum amount shall be the limited data set as provided in 45 CFR 164.514(e) or as otherwise provided by the Rule.

**4. Obligations of Participant:**

(A) Participant shall notify Forum of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Forum’s use or disclosure of PHI.

(B) Participant shall notify Forum of any restriction to the use or disclosure of PHI that Participant has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Forum’s use or disclosure of Protected Health Information, provided that Forum may cease to provide the Covered Services with regard to such patients.

(C) Participant shall notify Forum of any change to its Notice of Privacy Practice required by 45 CFR §164.520 that would affect Forum's compliance herewith.

(D) Participant shall not include any obligations and restrictions on the use, disclosure or request for PHI in Participant's Notice of Privacy Practices required by 45 CFR §164.520 that are inconsistent with Forum's Policies and Standards.

5. **Term:** This Agreement shall become effective on the effective date of the Contract and, except as hereinafter provided, shall remain in force and effect until the last of the PHI is returned to Participant or destroyed. Notwithstanding the forgoing, the rights and obligations provided by Sections 3(I), 10(B), 10(D), and 4 (to the extent that Forum has not returned or destroyed any portion of the PHI) shall survive indefinitely.

6. **Termination of Contract:** Notwithstanding any provision of the Contract to the contrary regarding term or termination, as hereinafter provided Participant is authorized to immediately terminate the Contract if it determines that Forum has violated a material term of this Agreement (a "Privacy Breach").

(A) If it is possible to cure the Privacy Breach, upon learning of a Privacy Breach, unless Participant reasonably believes that Forum has already cured the Privacy Breach (i.e., has remedied the condition leading to or causing the Privacy Breach), Participant shall give written notice thereof ("Notice") to Forum at the address listed in the Contract.

(B) If it is not possible to cure the Privacy Breach, or if Participant has not received satisfactory assurances within ten (10) days of the date of the Notice that Forum has cured the Privacy Breach, then Participant shall immediately terminate the Contract if, in Participant's sole discretion, it determines that termination is feasible. If Participant determines that termination is not feasible, it shall immediately report the problem to the Secretary of the Department of Health & Human Services.

7. **Conflicting provisions:** In the event that any requirements or provisions of this Agreement should be in conflict with any requirements or provisions of the Contract, the requirements or provisions of this Agreement shall control.

8. **Changes required by law:** The parties hereto have acknowledged that this Agreement is entered into in order to comply with the requirements of the Rule. In the event that the provisions or interpretation of the Rule are materially changed, or in the event that other law is enacted or interpreted which materially effects the terms of this Agreement, the parties agree to enter into a mutually acceptable amendment to this Agreement, on or before the effective date of that change, to bring the terms hereof into compliance therewith. In the absence of such an amendment, this Agreement shall be deemed to have been modified so as to continue to comply with Rule.

9. **Definitions:** As used in this Agreement, terms have the meanings set forth in the Rule.

10. **Miscellaneous:**

(A) **Ownership of PHI:** Except as otherwise provided in the Contract, the PHI to which Forum has access under the Contract or this Agreement shall not thereby become the property of Forum.

(B) **Indemnification:** Each party to this Agreement shall indemnify and hold the other harmless from any and all liability, damages, costs and expenses, including attorneys' fees and costs of defense, resulting from the action or omission of the other party.

(C) **Injunctive Relief:** Notwithstanding any rights or remedies provided for in this Agreement, Participant retains all rights to seek injunctive relief to prevent or stop the inappropriate use or disclosure of PHI directly or indirectly by Forum.

(D) **No Third Party Beneficiaries:** Nothing in this Agreement is intended to confer upon or create in, nor shall anything herein confer upon or create in, any person other than the parties and their successors and assigns, any rights, remedies, obligations, or liabilities whatsoever.

(E) **Choice of Law:** This Agreement shall be governed by the laws of the State of Louisiana.

(F) **Attorneys Fees:** If any legal action or other proceeding is brought for the enforcement of this Agreement or in connection with any of its provisions, the prevailing party shall be entitled to an award for the attorneys' fees and costs incurred therein in addition to any other right of recovery.

(G) **Amendment:** Except as provided in Article #8 on previous page, no amendment or other change to this Agreement shall be effective unless reduced to writing and signed by both parties hereto.

(H) **Severability:** In case any one or more of the provisions contained in this Agreement shall be invalid, illegal, or enforceable in any respect, the validity, legality, and unenforceability of the remaining provisions contained in this Agreement shall not be in any way affected or impaired.

(I) **Facsimile Signatures:** This Agreement may be executed and transmitted to the other party by facsimile, email or similar transmission technology and such copies shall have the same force and effect as the original.

**THUS DONE AND SIGNED** on the date first written above.

**Witnesses:**

**Participant:**

\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_  
By: \_\_\_\_\_  
Title: \_\_\_\_\_

**Witnesses:**

**Louisiana Health Care Quality Forum:**

\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_  
By: \_\_\_\_\_  
Title: \_\_\_\_\_

**EXHIBIT D**  
**FEE AND PAYMENT SCHEDULE**  
**[to be inserted]**

**EXHIBIT D-1**  
**FEES AND PAYMENT SCHEDULE**  
**[to be inserted]**

## **EXHIBIT E**

### **TECHNICAL ENVIRONMENT**

#### **A. Customer Technical Environment**

- Maintain Internet Connectivity and access to the Customers
- Access the SaaS Service through a web browser

#### **B. Data Source Description**

- Maintain internet connectivity for all data transmittals
- Maintain all source systems for all data transmittals

**EXHIBIT F**  
**LaHIE FEATURES AND FUNCTIONALITIES**

Core Functionality

- i. **Enterprise Master Patient Index** – An Enterprise Master Patient Index (EMPI) is used to manage patient identities across all LaHIE participants.
- ii. **Provider Registry** –The Provider Registry offers the capability to maintain a registry of physicians in Louisiana along with their local physician ID’s at each LaHIE participant
- iii. **User Identity Management and Authentication** - Provides secure, role based access to LaHIE.
- iv. **Audit Module** – LaHIE Audit Module provides HIPAA compliant tracking of access to all clinical information available via LaHIE.
- v. **Consent Management Module** –This module allows for the tracking and storage of a patient’s consent selection, either allowing or denying access to the patient’s record, according to their consent preference.
- vi. **Clinical Data Repository** – Provides Participants with a secure option for storing a sub-set of a patient’s record for view by authorized LaHIE Users.
  1. **Categories of Information Stored in CDR (as of Q1 2012):**
    - a. Demographics
    - b. Diagnostic Results including Lab, Radiology, Microbiology
    - c. Transcribed Reports including Discharge Summary, History & Physicals, Clinic Visit Summary
    - d. Known Problems and Allergies
    - e. Medications
    - f. Encounter Summary with admit and discharge diagnosis
    - g. Continuity of Care Record / Document (CCD / CCR)
- vii. **Clinical Portal** – Provides a web based clinical summary view of a Patient’s longitudinal medical record across all Participants.
- viii. **Direct Secure Messaging** – Provides Participants with a simple, secure, standards-based solution to send authenticated, encrypted health information directly to known, trusted recipients over the Internet. Information can be extracted from LaHIE, exported from a Participant EHR, or uploaded from a local device and sent securely to another Direct recipient.
- ix. **Public Health Reporting** – LaHIE works with the Louisiana Office of Public Health to facilitate required public health reporting on behalf of our Participants
  1. Participants have the following options:
    - a. Submit immunizations given by a Participant
    - b. Submit Syndromic Surveillance Data (Expect Production Q3 2012)

- c. Submit required Lab Results ( Expect Production Q3 2012)
  - d. Query immunization record (Expect Production in 2012)
- x. **Event Notification** – Health care providers sponsored by a Participant may elect to be notified when specific events occur for their patients
  - 1. These Events Include (as of Q1 2012?)
    - a. Admission to LaHIE Participant Emergency Department
    - b. In-Patient Admission to a LaHIE Participant Facility
    - c. In-Patient Discharge from a LaHIE Participant Facility
    - d. LaHIE receives a Diagnostic Lab Result
    - e. LaHIE receives a Diagnostic Microbiology Lab Result
    - f. LaHIE receives a Diagnostic Radiology Result
- xi. **Exchange of Data** – LaHIE gives Participants the ability to utilize our Enterprise Service Bus to facilitate the exchange of Patient Data between participant EHR systems
  - 1. Methods of Exchange
    - a. Send to my EMR – Gives LaHIE Users the ability to send a LaHIE generated CCD or Stored Lab result from LaHIE to the Participant EHR system
    - b. Event Notification Send to my EMR – Notification events will also be sent to Participant EHR System
    - c. Direct Secure Messaging – Send a CCD or Lab Result to any DIRECT secure messaging account from within Patient’s record in LaHIE
- xii. **Medicaid Eligibility** – Participants will be able to view Medicaid Eligibility status within a Patients Clinical record (Expect Production Q3 2012)

**EXHIBIT G**  
**SUPPLEMENTAL TERMS**



## 7.2 Email Authorization Dated December 2011

**From:** Jackson, Veronica (HHS/ONCIT) [mailto:Veronica.Jackson@hhs.gov]  
**Sent:** Monday, December 05, 2011 10:44 AM  
**To:** Jenny Smith; Joshua Hardy  
**Subject:** FW: State HIE Grant Program Clarification

Jenny and Josh,

I'm writing to confirm that you are approved to move the following initiatives to Phase 1 of your SOP:

- *Single sign-on capability so that providers can access LaHIE directly from their EMR without having to login separately to LaHIE – their login credentials and the context of any search they were conducting will pass securely from their EMR to LaHIE.*
- *Secure messaging via DIRECT. Secure messaging is currently enabled within the LaHIE solution, but the next step is for Orion to stand up their HISP and enable DIRECT.*
- *Connection to DHH for their required services, beyond the public health requirements for MU which we are already working toward. For instance, the large systems have communicated repeatedly that if we can automate the Medicaid eligibility verification process it will be a huge value-add for them and enable them to redirect current financial expenditures from other third parties to LaHIE, contributing to our long-term sustainability.*

As we've discussed, please provide additional detail regarding your proposal to connect HIE to HIE, as well as your Direct outreach strategy. This information will inform our decision to transition HIE to HIE exchange to another phase.

Best,  
Veronica

**Veronica E. Jackson**

Office of the National Coordinator for Health Information Technology  
U.S. Dept. of Health and Human Services  
330 C Street, SW, Suite 1100  
Washington, DC 20201  
202-205-7945 (Office)  
202-445-0588 (Cell)



## **7.4 LaHIE Policy Manual**

## LaHIE Policy Introduction

Establishing information sharing policies are among the most fundamental and critical decisions to be made for any effort to exchange or share health information, whether being pursued inside or outside of government. Coming to an agreement on workable policies requires broad, object involvement in order to get appropriate and relevant feedback and secure early buy-in as well as ongoing support for the initiative from various constituents and the public at large. Public trust will occur through both sound policies and an inclusive process, which also includes having consumers at the decision-making table. Since LHCQF's foundation is to have stakeholders input and involvement in all of its initiatives, the LaHIE policies were created and will be continuously reviewed and revised by various stakeholders throughout the state involved in LaHIE and health care legal and policy initiatives.

The Office of the National Coordinator for Health Information Technology (ONC) information regarding *Privacy and Security Framework Requirements and Guidance for the State Health Information Exchange Cooperative Agreement Program*, the Office of Civil Rights (OCR) information regarding the HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment in conjunction with *The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information* (the Privacy and Security Framework) and the Markle Foundation's *Connecting for Health Common Framework* were utilized as reference material in the development of these policies. These guidance illustrated how HIPAA covered entities may utilize the Privacy Rule's established baseline of privacy protections and individual rights with respect to individually identifiable health information to elicit greater consumer confidence, trust, and participation, in electronic health information exchange.

LaHIE and LHCQF with stakeholder involvement will review and update the Policy Manual at least annually to comply with changes in the law, including relevant standards and implementation requirements of HIPAA and the State of Louisiana.

## LOUISIANA HEALTH CARE QUALITY FORUM

<b>POLICY: : Access to LaHIE in accordance with HIPAA Privacy Rule</b>	<b>EFFECTIVE: 10-01-2011</b>
<b>DEPARTMENT: LHCQF; LaHIE</b>	<b>REVISED:</b>

### PURPOSE

To outline the protocol used to determine who has authorized access to LaHIE, both in data sharing and accessing the information.

### PROCESS

1. Access to LaHIE will only be provided to Participant organizations that have a signed Participation Agreement and Business Associate Agreement with LHCQF and are authorized to access data in accordance with HIPAA Privacy Rule.
2. Data shared with LaHIE on behalf of Participants/Providers will only be used for treatment and/or business operations as outlined in the HIPAA Privacy Rule. This may include submitting Participant/Provider information for public health reporting or to health oversight agencies at the state and federal level, i.e. immunizations, syndromic surveillance, registries, etc.
3. Payers (Insurance Providers) will not be given access to LaHIE at this time.
4. As defined by the HIPAA Privacy Rule, Participants as covered entities may use LaHIE to facilitate the exchange of PHI to other health care providers for treatment purposes, after initiation of the business associate agreement.
5. LaHIE may also receive PHI and manage, as a business associate on behalf of Participants, a master patient index for purposes of identifying and linking all information about a particular individual. Disclosures to, and use of, LaHIE for such purpose is permitted as part of the Participant's health care operations.

### APPROVAL:



---

Cindy Munn  
Executive Director  
Louisiana Health Care Quality Forum

## LOUISIANA HEALTH CARE QUALITY FORUM

<b>POLICY:</b> Accountability Principle in the Privacy and Security Framework	<b>EFFECTIVE:</b>
<b>DEPARTMENT:</b> LHCQF/LaHIE	<b>REVISED:</b>

### PURPOSE

To ensure a process is implemented, and adherences assured, through appropriate monitoring and other means and methods to report and mitigate non-adherence and breaches.

### PROCESS

1. Participating organizations as the covered entities that exchange protected health information (PHI) to and through LaHIE will comply with the HIPAA Privacy Rule administrative requirements and extend such obligations to LHCQF/LaHIE as a business associate.
2. Participating organizations as the covered entities are responsible for their own non-compliance with the HIPAA Privacy Rule, as well as that of their workforce.
3. LHCQF/LaHIE, through its business associate agreement with the participating organization, will be contractually obligated to adequately safeguard the PHI and to report noncompliance with the agreement terms to the participating organization/covered entity, and the covered entity will be held accountable for taking appropriate action to cure known noncompliance by LHCQF/LaHIE, the business associate, and if unable to do so, to terminate the business associate relationship.
4. LHCQF/LaHIE may provide satisfactory assurances as part of its business associate agreement that adequately safeguard PHI. These may include:
  - a. LaHIE will not use or disclose PHI except as allowed by the agreement
  - b. LaHIE will implement reasonable and appropriate safeguards for PHI
  - c. LaHIE will report any uses or disclosures of PHI that violate the agreement of the participant/covered entity.

### APPROVAL:



Cindy Muhn  
Executive Director  
Louisiana Health Care Quality Forum

## LOUISIANA HEALTH CARE QUALITY FORUM

<b>POLICY: LaHIE Audit Policy</b>	<b>EFFECTIVE: 10-01-2011</b>
<b>DEPARTMENT: LaHIE</b>	<b>REVISED:</b>

### PURPOSE

To outline the process of performing periodic reviews and verifications of audit logs for both operational monitoring and system security and to ensure compliance with all applicable regulations and laws.

### PROCESS

1. LHCQF's Health IT Director or designee of LaHIE is primarily responsible for execution and revision of the privacy and security policies, for ensuring audits occur by LaHIE staff and that results and corrective actions are undertaken and reported as appropriate. The Health IT Director or his/her designee will oversee the activities of LaHIE to evaluate compliance by Participants with this policy and enforce its terms.
2. An annual privacy and security internal audit plan will be developed by the Health IT Director or designee based on guidance from ONC and HIPAA regulations. This plan will receive input and direction from LHCQF's HIT Advisory Council and LHCQF's Board of Directors will be the governing body for final approval.
  - a. The audit plan will include the types of audits to be performed, the specific controls to be audited and the frequency and sample size for each audit.
  - b. Documentation of the audit and its results will be maintained and include the list of cases sampled for each audit, the audit schedule, and all audit activity.
3. Audit Process:
  - a. Audits will be conducted on a statistically significant sample size.
  - b. At least on an annual basis, or more frequently, as determined by the Health IT Director or designee, LaHIE will generate a random sample of records to be audited and work with the Participants to establish a process for review to establish the following with respect to each such record:
    - i. That any Authorized User who accessed Data of a Patient (1) executed the proper authorized user agreement and (2) had a treatment relationship with such Patient, or was authorized by the Participant to access such data.
4. Annually, the results of the privacy and security audits will be presented to the HIT Advisory Council for review and to LHCQF's Board of Directors for final approval.
5. Participants will have the responsibility to ensure compliance with state and federal laws and regulations, such as HIPAA, to maintain the confidentiality, privacy and security of individuals' protected health information. This includes ensuring that LaHIE is being used only for purposes authorized by the Participation Agreement, and that each individual who views data through LaHIE is doing so in a manner consistent with state and federal laws and regulations and privacy and security policies.

## LOUISIANA HEALTH CARE QUALITY FORUM

6. The LaHIE system will maintain audit trails. All user activity within the system is logged, enhancing audit capabilities and improving the general security of patient data. Audit trails of user logins, logouts, applications used, security overrides, patient selections and individual documents viewed are recorded, with the date and time. Audit log data is stored in a separate audit database.
7. If an audit reveals noncompliance by a Participant, a corrective action plan must be submitted by the Participant to the LHCQF Health IT Director or designee.
  - a. The Health IT Director or designee will forward the matter to the LHCQF Executive Director.
  - b. The Health IT Director or his/her designee will make a recommendation on the corrective action plan to LHCQF Executive Director as to whether a specified corrective action plan should be accepted as presented, be revised as per agreement reached by the Executive Director or be rejected.
  - c. If a corrective action plan is rejected, depending on the nature of the problem uncovered in the audit, the Executive Director after obtaining advice of Legal Counsel may decide to suspend access to the Exchange for either the Participant or one or more Authorized Users of such Participant until the problem is adequately addressed.
8. If an audit reveals noncompliance by a LHCQF staff, a corrective action plan must be submitted to the LHCQF Health IT Director or designee.
  - a. The Health IT Director or designee will forward the matter to the LHCQF Executive Director.
  - b. The Health IT Director or his/her designee will make a recommendation on the corrective action plan to LHCQF Executive Director as to whether a specified corrective action plan should be accepted as presented, be revised as per agreement reached by the Executive Director or be rejected.
  - c. If a corrective action plan is rejected, depending on the nature of the problem uncovered in the audit, the Executive Director after obtaining advice of Legal Counsel may choose to take necessary disciplinary action against the employee and suspend access to the Exchange for the employee until the problem is adequately addressed.

### APPROVAL:



---

Cindy Munn  
Executive Director  
Louisiana Health Care Quality Forum

## LOUISIANA HEALTH CARE QUALITY FORUM

<b>POLICY: Authorized Users Information and Types</b>	<b>EFFECTIVE: 10-01-2011</b>
<b>DEPARTMENT: LaHIE</b>	<b>REVISED:</b>

### **PURPOSE**

To outline the process used to designate the authorized users of LaHIE information and types of information that can be accessed.

#### **A. Authorized Users**

1. Participants are responsible for designating the "Authorized Users" within their organizations who will use the Exchange, including but not limited to employees and medical staff members.
2. Each Participant must designate the Privacy and/or Security Administrator and provide that persons' contact information to LaHIE.
3. The Security Administrator is responsible for identifying Authorized Users, assigning the appropriate security level for each Authorized User and obtaining organizational approval of proposed Authorized Users.
4. Each Participant and LaHIE shall have an authorization process in place to ensure users have access to only those applications and the protected health information that they are allowed to use or review.
5. LaHIE will accept requests for user IDs and passwords only from an organization's designated Security Administrator or personnel.
6. LHCQF may designate staff or support personnel as "Authorized Users" who will use LaHIE for maintenance, testing, training, and/or operations of LaHIE.
  - i. LHCQF will be responsible for assigning the user IDs and passwords and assigning the appropriate security level for each LHCQF Authorized User and obtaining organizational approval for proposed Authorized Users, i.e. Director of Health IT approval.

#### **B. Required Information for Authorized Users**

1. Access to the Exchange shall be based on the functional needs and job roles of each Authorized User.
2. Only the minimum access privileges necessary to perform a given job function should be requested by the Participant's Security Administrator, and only those will be granted by LaHIE.
3. The information required for each user access request includes:
  - i. First Name
  - ii. Last Name
  - iii. Title
  - iv. Password

## LOUISIANA HEALTH CARE QUALITY FORUM

- v. Company Name
  - vi. Job Category
  - vii. Office Phone
  - viii. Office Fax
  - ix. Office address
4. The following are only applicable to provider user requests:
- i. Cell phone
  - ii. Pager
  - iii. NPI (National Provider Identifier)
  - iv. Specialty
  - v. DEA Number

### C. Authorized User Types

1. Authorized Users are granted access to LaHIE functions based on their job category.
2. Participants shall limit Authorized User access to the minimum necessary required by the Authorized User's job category.
3. A Participant may define Authorized User job categories and access rights in accordance with the Participant's specific organizational needs and structure.
4. LaHIE reserves the right to review and approve the Participant-defined job categories and access rights.
5. To assist Participants in developing Authorized User job categories and access rights, LaHIE provides the following, non-exclusive recommendations:
  - i. *MD, DO, DDS, DPM, Resident and Nurse Practitioner*: Write and sign prescriptions. Access, review and edit patient clinical data.
  - ii. *Licensed Health Professional (PAs)*: Write and sign prescriptions for supervising MD's review. Access and review patient clinical data.
  - iii. *Staff 1*: Medical support of clinical staff members who need to draft prescriptions and/or access patient clinical data, after the patient record has been accessed in the clinical workgroup.
  - iv. *Staff 2*: Registration staff who have access only to demographic and health insurance eligibility information.
  - v. *Lab/Radiology Staff*: Lab and radiology technicians or support staff who will access patient demographics and clinical data for electronic ordering.
  - vi. *HIM Staff*: HIM professional or support staff will have full viewing right to demographic information and patient clinical data.
  - vii. *Designated Security Administrator*: Designated Security Administrator will have rights for identifying users, assigning the appropriate security level for each user and obtaining organizational approval of those users.
6. An Authorized User of LaHIE will be assigned a unique User ID, password and/or other security measures associated with and based on the specific user's role and job category. The users ID and passwords may not be shared with others.
7. The Authorized User's right to access clinical data through LaHIE will be terminated upon termination of the Authorized User's employment or relationship with the

## LOUISIANA HEALTH CARE QUALITY FORUM

Participant or upon any violation by the Authorized User of the Participation Agreement or the provisions of the Participant's Privacy and Security Policies or LaHIE's Policy Manual.

8. An Authorized Users' viewing rights will be defined by the Participants and defined by their role with the Participant. These may include:
  - i. Clinician with full viewing rights
  - ii. Other personnel with full viewing rights (to include only such individuals with need and reason to access clinical data who are authorized to access clinical data under applicable laws and regulations)
  - iii. Other personnel with limited viewing rights: these individuals will have access to only patient search and Participant's status screens in LaHIE.

### **D. Breaking the Glass:**

1. Only an Authorized User who is treating the patient may Break the Glass, i.e. access all of that patient's Confidential Health Information notwithstanding the absence of a Patient Choice Election Form or Patient Authorization Record permitting such access, if consent by or on behalf of the patient is not reasonably possible, and in the professional judgment of the Authorized User, access to such Confidential Health Information is necessary to ensure optimal Treatment of the patient. Notwithstanding the foregoing, an Authorized User may not access such information if the Patient Choice Election Form or Patient Authorization Record indicates that the patient elected not to participate in LaHIE.
2. Each time an Authorized User seeks access to a patient's Confidential Health Information under the circumstances detailed in the preceding paragraph, the Authorized User will be asked to certify that obtaining consent by or on behalf of the patient is not reasonably possible, and that, in the professional judgment of the Authorized User, access to such Confidential Health Information is necessary to ensure optimal Treatment of the patient. Authorized Users will not be permitted to access any Confidential Health Information without providing this certification.
3. Any access by an Authorized User to Confidential Health Information will be subject to an audit trail function that allows tracking and auditing of such access.

**E. Sensitive patient health information**, (e.g. HIV/AIDS, sexually transmitted diseases, substance abuse, mental health conditions), is restricted from access for most purposes. This information can only be accessed with patient's consent and under an "opening the privacy seal" access process and only by a clinician.

### **F. Termination of Access:**

1. An Authorized Users' access shall cease upon termination of that Authorized User by Participant.
2. Any Authorized Users failing to act in accordance with the Participation Agreement or LHCQF's policy manual will be disciplined.
  - i. Participant's Authorized Users may have their access temporarily disabled;
  - ii. Participant will be notified immediately of the concern or unauthorized access;
  - iii. LHCQF will coordinate solution with Participant to mutual agreement.

## LOUISIANA HEALTH CARE QUALITY FORUM

3. Designated LHCQF staff's access will be terminated upon termination of employment. In addition, staff's access will be temporarily disabled in accordance with LHCQF policies and the employee will be disciplined in accordance with LHCQF policies and procedures. Such disciplinary action may include termination.

For access descriptions, processes for "opening the privacy seal", and list of reasons for "breaking the glass", see *Users Permission Policy*.

### APPROVAL:



---

Cindy Munn  
Executive Director  
Louisiana Health Care Quality Forum

## LOUISIANA HEALTH CARE QUALITY FORUM

<b>POLICY: Compliance with Privacy and Security Laws and Protocol</b>	<b>EFFECTIVE: 10-01-2011</b>
<b>DEPARTMENT: LHCQF; LaHIE</b>	<b>REVISED:</b>

### PURPOSE

To outline the protocol used to maintain the confidentiality, privacy and security of individuals' protected health information in accordance with applicable state and federal regulations, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

### PROCESS

#### 1. Compliance with Privacy Laws, Regulations and Policies:

- a. All Participants must comply with state and federal laws and regulations, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), related to the use and disclosure of Confidential Health Information.
- b. LaHIE has implemented appropriate operational and technical safeguards to prevent the improper use and disclosure of Confidential Health Information. In the same way Participants must safeguard Confidential Health Information contained in records within their facility, they have the responsibility not to use or disclose information obtained through LaHIE inappropriately.

#### 2. Responsible Parties:

- a. LHCQF's Health IT Director is the designated LHCQF Privacy and Security Officer.
- b. LHCQF's Health IT Director or designee of LaHIE has primary responsibility for execution and revision of the privacy and security policies, for ensuring audits occur by LaHIE staff and that results and corrective actions are undertaken and reported as appropriate. The Health IT Director or his/her designee will oversee the activities of LaHIE to evaluate compliance by Participants with this policy and enforce its terms.
- c. An annual privacy and security internal audit plan will be developed by the Health IT Director or designee based on guidance from ONC and HIPAA regulations. This plan will receive input and direction from LHCQF's HIT Advisory Council and LHCQF's Board of Directors will be the governing body for final approval.
- d. Annually, the results of the privacy and security audits will be presented to the HIT Advisory Council for review and to LHCQF's Board of Directors for final approval.

## LOUISIANA HEALTH CARE QUALITY FORUM

- e. Participants will have the responsibility to ensure compliance with state and federal laws and regulations, such as HIPAA, to maintain the confidentiality, privacy and security of individuals' protected health information.

### 3. Business Associate Agreements:

- a. LaHIE will enter into a Participation Agreement with each Participant, which agreement shall include a Business Associate Agreement as required by 45 C.F.R § 164.502(e). LaHIE will ensure that all its contracts and contracts of any subcontracts include a Participation Agreement and/or Business Associate Agreement to the extent required by 45 C.F.R § 164.502(e).

### 4. Security Practices:

- a. Tracking. Any access by an Authorized User to Confidential Health Information through LaHIE will be subject to an audit trail function that allows tracking and auditing of such access.
- b. Confidentiality and Re-disclosure. Each Participant shall keep confidential any Confidential Health Information obtained through LaHIE and shall only re-disclose such Confidential Health Information as authorized by law.
- c. Virus Protection Software. Each Participant shall install, maintain and update virus protection software that meets minimum standards established by LaHIE as well as HIPAA regulations on all of its computers used for the purpose of accessing Confidential Health Information through LaHIE.
- d. Notification to LaHIE. Each Participant shall promptly notify LaHIE of any use or disclosure of Confidential Health Information in violation of this policy or any related security breach of which it becomes aware. Notwithstanding the foregoing, notification shall be made within 24 hours of actual knowledge. Each Participant shall, in consultation with LaHIE, take reasonable steps to mitigate the potentially harmful effects of any such incident.
- e. Additional Privacy and Security Measures. Participants shall adopt and implement any other privacy and security policies and procedures relating to the use, maintenance and disclosure of Confidential Health Information obtained through LaHIE that are necessary to assure the Participant's compliance with HIPAA and all other applicable confidentiality laws and regulations. Additionally, LaHIE and Participants will implement "reasonable and appropriate" safeguards to protect the security of PHI.

## LOUISIANA HEALTH CARE QUALITY FORUM

### 5. Participants Responsibility for Authorized User Compliance

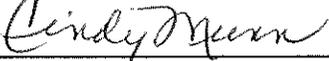
- a. Limits on Use. Confidential Health Information obtained by an Authorized User through LaHIE may be used or disclosed by the Authorized User for treatment or health care operations purposes only.
- b. HIPAA Training for Authorized Users. Each Participant is responsible for training of all its Authorized Users on compliance with this policy, the HIPAA regulations, other applicable privacy laws and rules and the Participant's privacy and security policies. Each Participant will require each Authorized User to execute an Authorized User Agreement. Authorized Users will include only those individuals who require access to LaHIE to facilitate use of the Data for a Permitted Use. Participant is responsible for its Authorized Users compliance with the terms and conditions of the Participation Agreement and applicable laws and regulations.
- c. Discipline for Violations. Each Participant shall be responsible for disciplining any of its Authorized Users who violate the terms of this policy, HIPAA or other applicable laws and regulations in accordance with its own policies and procedures. Notwithstanding the foregoing, LaHIE reserves the right, in its sole discretion, to terminate (or cause the applicable Participant to terminate) the access to LaHIE of any Authorized User who violates the terms of this policy, HIPAA or other applicable laws or regulations.
- d. Audits. LaHIE will conduct periodic audits of appropriate access to Confidential Health Information in accordance with LaHIE's audit policies. Participants are also encouraged to conduct periodic audits of appropriate access to their patient's Confidential Health Information in accordance with their privacy and security policies.

### 6. Access by LaHIE and LHCQF staff

- a. Notwithstanding anything to the contrary set forth in these Policies, LaHIE and LHCQF staff shall not have access to any Confidential Health Information through the LaHIE System other than in connection with the performance of audits in accordance with the Audit Policy, testing the functionality and operational support of LaHIE; provided that LaHIE/LHCQF staff's access to Confidential Health Information shall be limited only to such information as may be reasonably necessary for such auditing, testing and/or operational support functions.

LOUISIANA HEALTH CARE QUALITY FORUM

APPROVAL:

A handwritten signature in cursive script that reads "Cindy Munn". The signature is written in black ink and is positioned above a horizontal line.

---

Cindy Munn  
Executive Director  
Louisiana Health Care Quality Forum

## LOUISIANA HEALTH CARE QUALITY FORUM

<b>POLICY: Confidentiality and Security of Protected Health Information</b>	<b>EFFECTIVE: 10-01-2011</b>
<b>DEPARTMENT: LHCQF; LaHIE</b>	<b>REVISED:</b>

### PURPOSE

To outline the standards used to maintain the confidentiality, privacy and security of individuals' protected health information in accordance with applicable state and federal regulations, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

### RESPONSIBILITY

All LHCQF employees involved in the access, use, release or disclosure of an individual's protected health information (PHI). If a business partner has a different policy or contractual requirements, employees are expected to also comply with the business partner's policy or contractual requirements. This policy applies to LHCQF in its role as the business associate of HIPAA defined covered entities.

### PROCESS

#### A. Minimum Requirements

1. Reasonable efforts must be made to use, disclose or request only the minimum amount of PHI to accomplish the intended business objective.
2. Generally, only the narrowest or least amount of PHI is used or disclosed, covering the shortest period of time, to address the business objective for which the information is needed, and no more.
3. In addition, the use of PHI should be by, or disclosure should be to, only that person or those persons with a need-to-know, and who require the PHI to perform their functions or to accomplish a specific business objective.
4. When using or disclosing PHI for the following purposes, there is no minimum necessary requirement:
  - a. Treatment – disclosures to or requests by a healthcare provider for treatment to an individual;
  - b. Individual – permitted or required disclosures to, or requests by, an individual of his/her own information;
  - c. Authorized uses or disclosures – uses or disclosures authorized by an individual;
  - d. U.S. Department of Health and Human Services (HHS) – disclosures to HHS for investigation of HIPAA complaints;
  - e. Required by law – disclosures required by state or federal law; and
  - f. Compliance – uses or disclosures required for compliance with the HIPAA Administrative Simplification Rules.

## LOUISIANA HEALTH CARE QUALITY FORUM

### B. Uses and Disclosures of PHI

1. Uses and disclosures permitted with the individual's authorization:
  - a. An individual's PHI may be used or disclosed with the individual's (or individual's authorized personal representative's) authorization for any purpose. Such authorization from the individual must be documented.
2. Uses and disclosures permitted for payment or healthcare operations purposes that do not require the individual's authorization:
  - a. An individual's PHI may be used or disclosed without the individual's authorization for purposes of conducting the payment activities or healthcare operations of the covered entity when LHCQF is its business associate, or when the PHI is disclosed to LHCQF's business associate. The minimum necessary standard applies to these uses and disclosures.
  - b. The minimum necessary PHI may be disclosed to another covered entity (or at the direction of the covered entity) for the healthcare operations of the other covered entity if the PHI to be disclosed: (i) pertains to the relationship that both LHCQF (or the covered entity) have or had with the individual who is the subject of the PHI; and (ii) the healthcare operations for which the disclosure is being made involves one of the following:
    1. Quality assurance
    2. Competency assurance
    3. Fraud and abuse control
3. Uses and disclosures that require authorization from an individual:
  - a. Except for purposes of treatment, payment activities or healthcare operations, or as otherwise permitted or required by state or federal law, an individual's authorization must be requested prior to the use or disclosure of the individual's PHI.
  - b. An authorization is required to use or disclose PHI for marketing purposes that do not involve:
    - i. Communications about health-related products or services provided by, or included in a plan of benefits, or other value-added health-related products or services offered by the company;
    - ii. Distributing promotional items of nominal value; and
    - iii. Face-to-face communications by the company to the individual.
  - c. Activities requiring an authorization include those involving the use or disclosure of PHI maintained by LHCQF, such as brand name marketing, direct mail or telemarketing for non-health-related products or services (e.g., life

## LOUISIANA HEALTH CARE QUALITY FORUM

insurance, disability, etc.) or newsletters with articles about non-health-related products or services.

- d. An individual's authorization is required prior to the use or disclosure of an individual's psychotherapy notes (defined by HIPAA as notes recorded by a healthcare provider who is a mental health professional 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 individual's medical record).

### 4. De-identified health information

- a. There are no minimum necessary or authorization restrictions on the request for, or use or disclosure of, de-identified health information. PHI can be de-identified in one of two ways:

- i. Remove identifiers: if all of the following identifiers of the individual, his/her relatives, his/her employers or his/her household members are removed, and the employee using or disclosing the information has no actual knowledge that the information could be used alone or in combination with other information to identify an individual:
  - Names;
  - All elements of dates (except year) for dates directly related to an individual, including birth date, admission and discharge date, date of death, all ages over 89;
  - Telephone or fax numbers, e-mail addresses;
  - Social security numbers, medical record numbers, health plan beneficiary numbers, account numbers;
  - Certificate-license numbers, vehicle identifiers, device identifiers;
  - Web Universal Resource Locators (URLs), Internet Protocol (IP) address numbers;
  - Biometric identifiers, full face photographic images and any comparable images;
  - All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code; and
  - Any other unique identifying number, characteristic, or code (except re-identification codes).
- ii. Statistical method: It is determined that the risk is very small that the PHI could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is the subject of the PHI, based on generally accepted statistical and scientific principles and methods.

### 5. Disclosures permitted for purposes other than treatment, payment or healthcare operations

## LOUISIANA HEALTH CARE QUALITY FORUM

These disclosures do not require an authorization or other permission from the individual, but must meet the minimum necessary requirement and must be reported to LHCQF's Executive Director (or the customer's/covered entity's Privacy Officer) to be tracked for purposes of providing an accounting of disclosures:

- a. Health and safety purposes – disclosures to the extent necessary to avert a serious and imminent threat to an individual's health or safety of others, to a government agency authorized to oversee the healthcare system or government programs or its contractors, or to public health authorities.
- b. Public health activities – as permitted or required by law. For example, disclosures for the purposes of preventing or controlling disease, injury or disability; investigation of reportable diseases; the control of public health hazards; enforcement of sanitary laws; certification and licensure of health professionals and facilities; and review of healthcare that is required by the federal government and other governmental agencies.
- c. Health oversight activities – disclosure of PHI to a health oversight agency for activities authorized by law, such as audits, investigations, inspections, licensure or disciplinary actions, or civil, administrative, or criminal proceedings or actions.
- d. Required by law – PHI may be disclosed if required by law. There is no minimum necessary requirement for these disclosures.
- e. Legal, judicial and administrative proceedings – the minimum necessary PHI may be disclosed in response to a court or administrative order, subpoena, discovery request or other lawful process, in accordance with specified procedural safeguards. Subpoenas received for purposes other than health information management (HIM) routine operations should be referred to the LHCQF Legal Counsel.

### **C. Business Associates**

1. A business associate is a person or entity, other than a LHCQF employee, that performs or assists in performing, a function or activity that involves the use or disclosure of PHI on behalf of LHCQF.
2. LHCQF contracts with business associates and also functions as the business associate of other covered entities.
3. Prior to the disclosure of PHI to a business associate, or prior to the business associate being allowed to create or receive PHI, "satisfactory assurances" will be obtained in the form of a written agreement that the business associate will appropriately safeguard and limit their use and disclosure of the PHI.

## LOUISIANA HEALTH CARE QUALITY FORUM

4. The LHCQF Legal Counsel must review all business contracts to determine whether business associate requirements should be added to the contract.

### D. Individual Rights

Requests for the following individual rights will be coordinated by LHCQF's Executive Director or at the direction of the covered entity's Privacy Officer:

1. Access – Individuals have the right to inspect and obtain a copy of the PHI contained in their designated record set for as long as the information is maintained. Designated record set is defined as a group of records maintained by LHCQF or its business associates, which is used to make treatment decisions about individuals.
2. Amendment – Individuals have the right to request amendment of their PHI and other records contained in their designated record set for as long as the designated record set is maintained. *See Correction Policy*
3. Accounting of disclosure – Individuals have the right to an accounting of the disclosures of PHI that were made after April 14, 2003, for purposes other than treatment, payment or healthcare operations, or other than pursuant to a valid authorization when such authorization is required. It is the responsibility of the Compliance Department (or covered entity's Privacy Office) to ensure that each disclosure made that is not exempted from the accounting requirement is documented. *See Correction Policy*
4. Restriction on use or disclosure – Individuals have the right to request that the use or disclosure of their PHI be restricted, including uses and disclosures made for treatment, payment or healthcare operations. LHCQF does not have an obligation to agree to the request, but if agreed to, LHCQF will comply with the agreement and notify any business associates of such agreement. *See Correction Policy*
5. Confidential communications – Individuals have the right to request that LHCQF use alternative means or alternative locations (street address and/or telephone number) when communicating PHI to them.

### F. Complaint Management

1. Any workforce member who suspects that the privacy or security policies and procedures, the HIPAA privacy or security rules, or other applicable federal or state privacy laws have been violated must report the suspicion to the Executive Director in sufficient detail to permit the matter to be investigated and to prevent or mitigate any deleterious effects.
2. All privacy and security complaints will be fully investigated, and appropriate actions taken, including, but not limited to:
  - i. Technical system modifications;
  - ii. Modifying or expanding audits;
  - iii. Re-educating staff; and/or

## LOUISIANA HEALTH CARE QUALITY FORUM

- iv. Strengthening departmental procedures.
3. Employees that violate the privacy or security policies, the HIPAA privacy or security rules, or other applicable federal or state laws will be subject to disciplinary action as outlined in the LHCQF Employee Manual. The LHCQF Executive Director will act promptly to mitigate, to the extent possible, any harmful effect of improper use or disclosure of PHI.

### G. Employee Training and Management

1. Orientation and training
  - a. All new hires are given information on LHCQF's Code of Corporate Conduct and LHCQF's Employee Manual.
  - b. New hires must complete the LHCQF training program, which contains training on HIPAA privacy and security, within 60 days of hire.

2. Access to information
  - a. Workforce members authorized to have access to PHI (and electronic PHI) to perform their job functions shall have access only to that level of information necessary to complete their job functions.

3. Documentation and retention

LHCQF will maintain in written or electronic form for six years from the date of creation or last effective date, whichever is later:

- a. LHCQF's privacy and security policies and each revision of them;
- b. Each request from individuals for access, amendment, disclosure accounting, restriction or confidential communications and all documentation relating to them;
- c. Each complaint related to a real or perceived privacy or security violation and supporting documentation; and
- f. Other documentation requested or required by state or federal law, or this policy.

#### APPROVAL:



---

Cindy Munn  
Executive Director  
Louisiana Health Care Quality Forum

LOUISIANA HEALTH CARE QUALITY FORUM

<b>POLICY: Correction Policy</b>	<b>EFFECTIVE: 140-01-2011</b>
<b>DEPARTMENT: LaHIE</b>	<b>REVISED:</b>

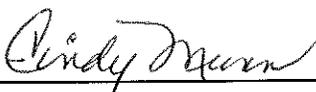
**PURPOSE**

To provide individuals with a timely means for patient corrections within the Health Information Exchange, including the ability to dispute the accuracy or integrity of their individually identifiable health information and to have erroneous information corrected or to have a dispute documented if their requests are denied.

**PROCESS**

1. Individuals have the right to have their protected health information (PHI) amended in a manner that is fully consistent with the Correction Principle in the Privacy and Security Framework. (See 45 C.F.R § 164.526.)
2. The HIPAA Privacy Rule designated the Participant/covered entity as the responsible party for acting on an amendment or correction request from an individual/patient.
3. LaHIE, acting as a business associate of the covered entity, can assist the covered entity in informing other Participants in LaHIE who are known to have the individual's information, of the amendment by efficiently disseminating amended information to appropriate recipients throughout the electronic exchange.
4. Participants must take action in a timely manner, usually within 60 days, to correct the record as requested, with an additional 30 day extension in certain circumstances, or to notify the person if the request is denied.
5. A request may be denied if the Participant determines that the information is complete and accurate, and on limited other grounds.
6. When a request is denied, but the individual continues to dispute the accuracy of the information, the individual must be provided an opportunity to file a statement of disagreement with the covered entity and the covered entity must provide documentation of the dispute with any subsequent disclosure of the disputed PHI.
7. Through LaHIE, the covered entity should be able to identify other Participants that maintain information on the individual and who, therefore, should be notified of the amended information.

**APPROVAL:**

  
\_\_\_\_\_  
Cindy Munn  
Executive Director  
Louisiana Health Care Quality Forum

## LOUISIANA HEALTH CARE QUALITY FORUM

<b>POLICY: Corrective Action Policy</b>	<b>EFFECTIVE: 10-01-11</b>
<b>DEPARTMENT: LaHIE</b>	<b>REVISED:</b>

### PURPOSE

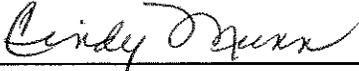
To outline the process to be taken as corrective action upon identification and/or notification of noncompliance, either by a Participant or staff of LHCQF.

### PROCESS

1. According to LaHIE policy ("LaHIE Audit Policy"), if an audit reveals noncompliance, a corrective action plan must be submitted by the Participant to the LHCQF's Health IT Director or designee.
  - a. The Health IT Director or designee will forward the matter to the LHCQF Executive Director.
  - b. The Health IT Director or his/her designee will make a recommendation on the corrective action plan to LHCQF Executive Director as to whether a specified corrective action plan should be accepted as presented, be revised as per agreement reached by the Executive Director or be rejected.
  - c. If a corrective action plan is rejected, depending on the nature of the problem uncovered in the audit, the Executive Director after obtaining advise of Legal Counsel may decide to suspend access to the Exchange for either the Participant or one or more Authorized Users of such Participant until the problem is adequately addressed.
  
2. If an audit reveals noncompliance by a LHCQF staff, a corrective action plan must be submitted to the LHCQF's Health IT Director or designee.
  - a. The Health IT Director or designee will forward the matter to the LHCQF Executive Director.
  - b. The Health IT Director or his/her designee will make a recommendation on the corrective action plan to LHCQF Executive Director as to whether a specified corrective action plan should be accepted as presented, be revised as per agreement reached by the Executive Director or be rejected.
  - c. If a corrective action plan is rejected, depending on the nature of the problem uncovered in the audit, the Executive Director after obtaining advise of Legal Counsel may choose to take necessary disciplinary action against the employee and suspend access to the Exchange for the employee until the problem is adequately addressed.

LOUISIANA HEALTH CARE QUALITY FORUM

APPROVAL:

A handwritten signature in cursive script, appearing to read "Cindy Munn", is written above a horizontal line.

Cindy Munn  
Executive Director  
Louisiana Health Care Quality Forum

## LOUISIANA HEALTH CARE QUALITY FORUM

<b>POLICY:</b> Data Breach Notification and Investigation	<b>EFFECTIVE:</b> 10-01-2011
<b>DEPARTMENT:</b> LHCQF; LaHIE	<b>REVISED:</b>

### PURPOSE

To facilitate compliance with the Health Information Technology for Economic and Clinical Health Act (HITECH) component of the American Recovery and Reinvestment Act of 2009 (ARRA) breach notification and investigation of unsecured protected health information (PHI) requirements.

### DEFINITIONS

The following definitions apply to all of LHCQF's privacy and security policies and procedures:

1. **Breach** – Unauthorized acquisition, access, use, or disclosure of unsecured, unencrypted protected health information which compromises the security or privacy of such information and poses a significant risk of financial, reputational, or other harm to the individual. To determine if a notification is required, a risk assessment must be performed to determine if the security or privacy of the PHI has been compromised (see Appendix A). The term 'breach' does not include:
  - a. Any unintentional acquisition, access, or use of PHI by a workforce member or individual acting under the authority of a covered entity or business associate if
    - i. Such acquisition, access, or use was made in good faith and within the course and scope of authority;
    - ii. Such information is not further used or disclosed in a manner not permitted; or
    - iii. Any inadvertent disclosure by a person who is authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates; and any such information received as a result of such disclosure is not further used or disclosed in a manner not permitted; or
    - iv. A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
2. **Protected Health Information** – Any oral, written or electronic individually-identifiable health information collected or stored by a covered entity or business associate. Individually-identifiable health information includes demographic information and any information that relates to past, present or future physical or mental condition of an individual.
3. **Unsecured PHI** - Protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology

## LOUISIANA HEALTH CARE QUALITY FORUM

specified by the U. S. Secretary of the Department of Health and Human Services (HHS). At this time, the only technology is encryption; the only methodology is destruction.

### PROCESS

1. Any Participant and/or LHCQF employee and/or support personnel in the case of a breach of unsecured PHI must notify LHCQF Executive Director or designee upon suspicion or knowledge of a breach within 24 hours.
2. If notification is received from a LHCQF employee or support personnel and the breach involves a customer's PHI, the Executive Director shall coordinate with the appropriate LHCQF Client Executive to provide notification to the customer's Compliance and/or Privacy/Security Officer without unreasonable delay.
3. A breach is considered discovered as of the first day on which the breach is known by the Participant and/or LHCQF employee or support personnel.
4. If a law enforcement official determines that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, such notification, notice or posting shall be delayed in the same manner as provided under §164.528(a)(2) of title 45, Code of Federal Regulations.
5. If a data breach occurs involving a customer's PHI, LHCQF's Executive Director or her designee will provide the same information as in the Content of Notification (below) to the customer's Compliance and/or Privacy Officer without unreasonable delay for completion of the risk assessment and determination of notification.
6. Participants and LHCQF/LaHIE are responsible for immediately investigating and mitigating to the extent possible, any privacy and/or security breach that they become aware of. They shall immediately:
  - a. Investigate the scope and magnitude of the breach.
  - b. Identify the root cause of the breach.
  - c. Mitigate the breach to the extent possible.
  - d. Notify all appropriate parties, i.e. LHCQF Executive Director, Participant's Privacy and Security Officers, etc., within 24 hours of actual knowledge and the potential impact of the breach.
  - e. In the event that the breach involves or may involve more than one Participant, Participants shall cooperate with LaHIE and other Participant(s) in investigating and mitigating the breach, including but not limited to sharing any information that may be

## LOUISIANA HEALTH CARE QUALITY FORUM

necessary in connection with such investigation and/or mitigation, subject to all applicable laws and regulations.

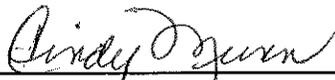
- f. Notify regulatory agencies and customers in compliance with all applicable state and federal laws, rules and regulations.
  - g. Notify individuals affected by the breach as required by HIPAA.
7. LHCQF Health IT Director will provide a report of the breach and mitigation actions to the LHCQF Executive Director, its Legal Counsel, and LHCQF Board of Directors.
  8. LHCQF shall maintain a log of any breaches meeting the HITECH definition that occur during a calendar year. This documentation must be retained for a period of six years.

### Content of Notification

The notice of the breach must include:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
2. A description of the type of unsecured PHI that were involved in the breach, such as full name, Social Security Number, date of birth, home address, account number, diagnosis code or disability code. Only the generic type of PHI should be listed in the notice (i.e., date of birth rather than the patient's actual birth date).
3. The steps the individual should take to protect themselves from potential harm resulting from the breach.
4. A brief description of what LHCQF is doing to investigate the breach, mitigate harm to the individual, and to protect against further breaches.
5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free number, an e-mail address, website, or postal address.

### APPROVAL:



---

Cindy Munn  
Executive Director  
Louisiana Health Care Quality Forum

## LOUISIANA HEALTH CARE QUALITY FORUM

### **GENERAL BREACH PROCESS INFORMATION FOR COVERED ENTITIES**

#### **Breach Notification Process**

##### **Patient Notification**

1. After a complete investigation, no later than 60 days from breach discovery, the covered entity must provide written notice to the patient or:
  - a. If the patient is deceased, the next of kin or personal representative.
  - b. If the patient is incapacitated/incompetent, the personal representative.
  - c. If the patient is a minor, the parent or guardian.
2. Written notification must be in plain language at an appropriate reading level with clear syntax and language with no extraneous materials. Americans with Disabilities Act (ADA) and Limited English Proficiency (LEP) requirements must be met.
3. Written notification must be sent to the last known address of the patient or next of kin, or if specified by the patient, by encrypted electronic mail. The template letter in the HITECH Breach Notification Reporting Process must be used when sending written notification to a patient, personal representative, or next of kin.
4. In the case where there is insufficient or out-of-date contact information:
  - a. For less than ten (10) individuals that precludes direct written notification to the patient, a substitute form of notice shall be provided such as telephone call.
  - b. In the case that there are ten (10) or more individuals for which there is insufficient or out-of-date contact information and contact information is not obtained, the covered entity must:
    - i. Post a conspicuous notice for 90 days on the homepage of their website that includes a toll-free number; or
    - ii. Provide notice in major print or broadcast media in the geographic area where the patient can learn whether or not their unsecured PHI is possibly included in the breach. A toll-free number must be included in the notice.
5. If the covered entity's Compliance Officer, in concert with the Legal Department/Team, determines a patient should be notified urgently of a breach because of possible imminent misuse of unsecured PHI, the covered entity may, in addition to providing notice as outlined in steps 2-4 above, contact the patient by telephone or other means, as appropriate.

##### **Media Notification**

1. In the case where a single breach event affected more than 500 residents of the same State or jurisdiction, notice shall be provided to prominent media outlets. A jurisdiction is defined as a geographic area smaller than a state (e.g., city, county). For example, if a single breach event

## LOUISIANA HEALTH CARE QUALITY FORUM

affects 200 patients in Texas and 400 patients in Louisiana, a notice to the media is not required because there were not more than 500 patients in the same State or jurisdiction affected. However, if a single breach event affects 500 patients in Texas and 500 patients in Louisiana, a media notice is required in both Texas and Louisiana.

2. The covered entity's Compliance Officer shall work with the Legal Department/Team and the Chief Executive Officer to coordinate the notification.

### HHS Notification

1. Notice must be provided by the covered entity without reasonable delay and in no case later than 60 days from the breach discovery to the U. S. Secretary of the Department of Health and Human Services (HHS) if a single breach event was with respect to 500 or more individuals regardless of the State or jurisdiction. The covered entity must use the electronic form available on the HHS website when notifying HHS of breaches involving 500 or more individuals.
2. If a breach is with respect to less than 500 individuals, the covered entity must use the electronic form available on the HHS website and submit to HHS no later than 60 days after the end of the calendar year in which the breach occurred.
3. The covered entity must maintain a log of any breaches meeting the HITECH definition that occur during a calendar year. This documentation must be retained for a period of six years.

# LOUISIANA HEALTH CARE QUALITY FORUM

## APPENDIX A

### Assessment of the Risk of Harm to the Individual

#### from a Violation of the Privacy Rule under HIPAA and the HITECH Act

Violations of the HIPAA Privacy Rule are evaluated for the potential for significant risk of financial, reputational, or other harm to the individual whose information was compromised. This risk assessment is completed and documented for every violation of the Privacy Rule involving unauthorized acquisition, access, use or disclosure of unsecured PHI that does not fit within an exception defined in the HITECH Act. When a violation is determined to result in significant risk of harm to the individual, notification to the individual and to the Secretary of HHS is required.

The following general framework is used to assess for risk depending upon the specific facts associated with the risk in order to determine whether breach notification is required.

#### 1. Who are the parties involved in the incident?

##### a. Is the individual who impermissibly used/disclosed the information an LHCQF employee?

Lo	(1)	LHCQF employee otherwise authorized to access the PHI
Lo	(1)	LHCQF employee not otherwise authorized to access the PHI
Med	(2)	Non LHCQF employee accessed/used/disclosed the PHI

##### b. Who received the disclosed PHI?

Lo	(1)	Another LHCQF employee not defined in the exceptions to breach
Lo	(1)	An individual that is a covered entity or a business associate
Med	(2)	An individual that is not bound by HIPAA and external to LHCQF

#### 2. What type(s) of information was disclosed?

##### a. Limited Data Set

N/A	(0)	Not a Limited Data Set
Lo	(1)	16 HIPAA defined identifiers removed and also either no date of birth (DOB) or no zip code
Lo	(1)	16 HIPAA defined identifiers removed and age or zip codes do not create identifiable populations
Med	(2)	16 HIPAA defined identifiers removed, but ages or zip codes make re-identification possible

**LOUISIANA HEALTH CARE QUALITY FORUM**

**b. Direct Patient Identifiers**

	N/A	(0)	No direct identifiers were disclosed
	Lo	(1)	Full name or partial name, but no contact demographic information (such as address or phone), may include medical record number but no Social Security number (SSN) or DOB
	Med	(2)	Name with phone number or address but no SSN or DOB
	Med	(2)	Full name with DOB
Mandatory	HI	(3)	SSN (or credit card or bank account number) with first initial or first name and last name

**c. Type of services provided**

	N/A	(0)	No information regarding health services or care disclosed
	Lo	(1)	Identified as patient of an LHCQF customer or customer's provider
	Med	(2)	Reason for receiving care; diagnosis or treatment; or test results disclosed
Mandatory, if any of 21b applies	HI	(3)	"Sensitive" treatment revealed by location or a condition that might result in employment discrimination or reputational harm (e.g. HIV, Cancer, Substance Abuse, genetic disorders)

**3. What is the likelihood of unauthorized use or disclosure of the PHI?**

**a. Lost or Stolen Device with ePHI**

N/A	(0)	Not applicable
Lo	(1)	Device retrieved before it was accessed or device encrypted
Med	(2)	Device is known to be password protected but not encrypted
HI	(3)	Device not known to be encrypted

**b. Paper Media Breached (e.g. lost, stolen, faxed, or mailed)**

N/A	(0)	Not applicable
Lo	(1)	Information is returned without seal on envelope being broken
Med	(2)	PHI is disclosed to someone who does not know the patient and who provides assurance the information has been returned and/or destroyed
HI	(3)	PHI is disclosed to someone who may know of the patient and who is reasonably believed to have accessed the information

LOUISIANA HEALTH CARE QUALITY FORUM

Risk Assessment Scoring Grid

Question	Score	Notes
1 a.		
1 b.		
2 a.		
2 b.		
2 c.		
3 a.		
3 b.		
<b>TOTAL</b>		
<b>KEY:</b>	0-7	Low Risk of Harm to the Individual (notification not required)
	8 – 9	Medium Risk of Harm to the Individual (notification may be required; determined by business leader and Privacy Office based upon facts of specific event)
	10 or more	High Risk of Significant Harm (notification will generally be required unless an exception is determined based upon specific facts of the event)
	2-b: HI	Automatically triggers notification requirements under federal law (and possible State law)
	2-c: HI	Automatically triggers notification if any 2-b direct identifiers are also disclosed

Completed by:

Date:

## LOUISIANA HEALTH CARE QUALITY FORUM

<b>POLICY: Enterprise Master Patient/Person Index Maintenance</b>	<b>EFFECTIVE: 10-01-2011</b>
<b>DEPARTMENT: LaHIE</b>	<b>REVISED:</b>

### PURPOSE

To ensure a process is implemented and followed to maintain the Enterprise Master Patient/Person Index (EMPI) and perform all duties necessary for ensuring the integrity and quality of the EMPI data.

### PROCESS

#### 1. Patient Matching

- a. LHCQF, in conjunction with the EMPI Software vendor, will establish the matching thresholds to be used. These thresholds, along with industry standard matching algorithms, are used to identify the incoming and existing records that should be linked. LaHIE staff will monitor the matching results, and make periodic adjustments to the thresholds as necessary.
- b. The EMPI Software vendor utilizes a proprietary algorithm to assess the similarity of individual records. When two records are compared, the algorithm generates a weighting that describes how similar the two records are. If this weighting falls below a Duplicate Threshold level, the records are treated as separate and no further actions are taken. If the weighting falls between the Duplicate Threshold and the Match Threshold, the system flags these records as being potential duplicates, and requires further manual intervention. If the weighting falls above the Match Threshold, the system automatically merges the two records, unless the records are flagged as potential false positives by the system, requiring further manual intervention. An example of a potential false positive is where two records are almost identical (as in the case of twins) resulting in a high weighting score, but the two records should remain unique. The algorithm considers certain demographic fields contained in a record - such as First Name, Last Name, Social Security Number, Date of Birth, Gender, etc. - and applies a weighting corresponding to how similar the two fields are to each other. Specific information regarding the Duplicate and Match Thresholds, field weightings, and other algorithm and matching-specific information can be found in the LaHIE EMPI Settings document.

#### 2. Unresolved Matches

- a. LHCQF, in conjunction with Participants' HIM Director (or their designee), will establish procedures to correct any unresolved matches or discrepancies within the EMPI. Timeframes for resolution will be agreed to by all parties involved in establishing the procedure. The procedure and timeline for resolution will be reviewed periodically, and adjusted as necessary.

#### 3. Access to EMPI

- a. LHCQF's Health IT Director, or designee, must authorize access to the EMPI System. Direct access to the EMPI System will be granted to staff members, sub-contractors, EMPI software vendor, etc. as necessary to maintain the quality and integrity of the EMPI. Additional access will have to be approved by the Health IT Director or their

## LOUISIANA HEALTH CARE QUALITY FORUM

designee. The Health IT Director will periodically review the list of authorized users and remove users who will no longer be requiring access to maintain the EMPI.

4. Matching Process Audit
  - a. LHCQF will periodically perform audits on a sample set of records after they have been processed by the matching algorithm within the EMPI. This sample set will be compared to established matching thresholds to confirm the algorithm is functioning as configured.
5. Accuracy Threshold
  - a. LHCQF will implement processes to ensure an accuracy threshold of at least 95% is achieved in patient matching approach.

### APPROVAL:



---

Cindy Munn  
Executive Director  
Louisiana Health Care Quality Forum

## LOUISIANA HEALTH CARE QUALITY FORUM

<b>POLICY: Individual Access to PHI</b>	<b>EFFECTIVE: 10-01-2011</b>
<b>DEPARTMENT: LHCQF/LaHIE</b>	<b>REVISED:</b>

### PURPOSE

To ensure a process is implemented that allows individuals the right to access their protected health information (PHI), right to amend their PHIE, and accounting of disclosures of PHI.

### PROCESS

1. Participating organizations as the covered entities that exchange protected health information (PHI) to and through LaHIE will comply with the HIPAA Privacy Rule administrative requirements and extend such obligations to LHCQF/LaHIE as a business associate.
2. Participants as covered entities under the HIPAA Privacy Rule will have the opportunity to enable patients to have the right to make requests for access to their PHI, provided they inform individuals of such a requirement. (See 45 C.F.R. § 164.524(b)(2)(i).)
3. Participants shall develop and implement reasonable policies and procedures that outline the specific provisions of access, form or format of access provided, and denial of access process.
4. LHCQF/LaHIE may be permitted by the Participant/covered entity, acting as its business associate, to assign the appropriate credentials and authenticate personal representatives, and any others, seeking access to PHI.
5. Participants shall educate patients with respect to the terms and conditions upon which their health information is shared and their rights to access their own health information.
6. Patient access to health information must be in accordance with all applicable laws and regulations, included but not limited to, La. R.S. 40:1299.96(A)(2)(d) which allows a health care provider to deny access to a record if the health care provider reasonably concludes that knowledge of the information contained in the record would be injurious to the health or welfare of the patient or could reasonably be expected to endanger the life and safety of any other person, La. R.S. 40:1300.14 regarding confidentiality of HIV patients, and any and all state and federal laws permitting denial of access to medical information in specific circumstances.

### APPROVAL:



Cindy Munn  
Executive Director  
Louisiana Health Care Quality Forum

## LOUISIANA HEALTH CARE QUALITY FORUM

<b>POLICY: Individual Choice for Sharing Information in LaHIE</b>	<b>EFFECTIVE: 10-01-2011</b>
<b>DEPARTMENT: LaHIE</b>	<b>REVISED:</b>

### PURPOSE

To provide guidelines defining the process of how individuals should be provided a reasonable opportunity and capability to make informed decisions about the use and disclosure of their individually identifiable health information as it relates to the Louisiana Health Information Exchange (LaHIE) and in alignment with the HIPAA Privacy Rule as it relates to the Individual Choice Principle in the Privacy and Security Framework.

### PROCESS

1. As a HIPAA covered entity, each Participant that intends to electronically exchange protected health information (PHI) to and through LaHIE, primarily for the purpose of treatment, will focus on how the Privacy Rule's provisions for optional consent and the right to request restrictions on certain uses and disclosures can support and facilitate individual choice with respect to the electronic exchange of health information in a networked environment.
2. Commencing the effective date of the Participation Agreement, each Participant that is providing data may elect to adopt an individual consent policy and, as part of the patient admission/registration process, offer each individual/patient the opportunity to make *meaningful choices* with respect to the electronic exchange of their individually identifiable health information.
3. A patient's *meaningful choice* means that choice is:
  - a. Made with advance knowledge/time;
  - b. Note used for discriminatory purposes or as condition for receiving medical treatment;
  - c. Made with full transparency and education;
  - d. Commensurate with circumstances for why PHI is exchanged;
  - e. Consistent with patient expectations; and
  - f. Revocable at any time.
4. Once an individual/patient has indicated his/her choice to participate in LaHIE or not, the Participant is responsible for creating a record of the individual/patient's choice.
5. The Participant is responsible for noting in the LaHIE system the individual/patient's choice and assuring that the presence of an appropriate Patient Authorization Record is maintained.
6. If obtained, each Participant must maintain documentation of each individual/patient's decision to participate or not participate in LaHIE.
7. If the Patient Authorization Record indicates that the individual/patient has chosen to participate in LaHIE, the individual/patient's Confidential Health Information will be exchanged.
8. The Privacy Rule also provides individuals/patients with a right to request that a covered entity restrict uses or disclosures of PHI about the individual for treatment, payment, or health care operations purposes. Covered entities are not required to agree to an individual/patient's request for a restriction, however, they are required to have policies in place by which to accept or deny such requests.
9. An individual/patient may not designate that some Confidential Health Information will be shared through LaHIE, while other information will not. If an individual/patient specifies he/she

## LOUISIANA HEALTH CARE QUALITY FORUM

does not wish to have particular Confidential Health Information shared through LaHIE, all information on that patient will be blocked from view through LaHIE.

10. Notwithstanding anything to the contrary set forth in these Policies and Procedures, Participants may disclose individual/patient demographic information to LaHIE even if an individual/patient chooses not to participate in LaHIE.
11. An individual/patient who has opted out of having his or her Health Information available through LaHIE may choose at a later time to have his or her Health Information shared in LaHIE, the individual/patient (or that individual's/patient's representative) must request, in a form or manner determined by the Participant, that the individual's/patient's Health Information be updated to reflect new status made available through LaHIE. If an individual/patient chooses to participate in LaHIE, all available information regarding the individual/patient may be accessed through LaHIE.

### APPROVAL:



---

Cindy Munn  
Executive Director  
Louisiana Health Care Quality Forum

## LOUISIANA HEALTH CARE QUALITY FORUM

<b>POLICY: Information Subject to Special Protection</b>	<b>EFFECTIVE: 10-01-2011</b>
<b>DEPARTMENT: LaHIE/LHCQF/LHIT Resource Center</b>	<b>REVISED:</b>

### PURPOSE

This policy promotes the privacy principles of purpose specification and minimization, security safeguards and controls, use limitation, data integrity and quality, collection limitation, and individual participation and control, particularly as it facilitates individualized privacy protections by requiring Participants to heed any special protections of certain information set forth under applicable laws. IN complying with these special protections, Participants' collection, use and disclosure of health information is limited to legitimate purposes.

### PROCESS

1. Some health information may be subject to special protection under federal, state, and/or local laws and regulations (e.g. substance abuse, mental health, and HIV).
2. Each Participant shall determine and identify what information is subject to special protection under applicable law prior to disclosing that information through LaHIE.
3. Each Participant is responsible for complying with such laws and regulations.
4. Sensitive patient health information, (e.g. HIV/AIDS, sexually transmitted diseases, substance abuse, mental health conditions), that is shared with LaHIE is still restricted from access for most purposes. This information can only be accessed with patient's consent and under an "opening the privacy seal" access process and only by a clinician.
5. Sensitive patient information is applied based on specific blocked codes. *Refer to Orion listing of protected codes for the specific blocked codes.* This applies to:
  - i. Lab/Micro results (LOINC)
  - ii. Medications (RxNorm)
  - iii. Problems (ICD-9-CM)
  - iv. Encounters (Diagnosis ICD-9-CM Code)
  - v. Procedures (CPT codes)
6. The rules around who can see sensitive data:
  - i. Level 1 Provider – Privacy Sealed Access only
  - ii. All other users – No access.

### APPROVAL:



Cindy Murfin  
Executive Director  
Louisiana Health Care Quality Forum

## LOUISIANA HEALTH CARE QUALITY FORUM

<b>POLICY: LaHIE Data Quality and Integrity</b>	<b>EFFECTIVE: 10-01-2011</b>
<b>DEPARTMENT: LHCQF/LaHIE</b>	<b>REVISED:</b>

### **PURPOSE**

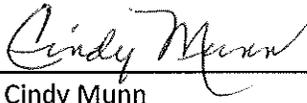
To ensure a process is in place to ensure individually identifiable health information (IIHI) is complete, accurate and up-to-date to the extent necessary for the Participant's or entity's intended purpose and has not been altered or destroyed in an unauthorized manner.

### **PROCESS**

1. LaHIE, in the role of the information conduit, does not possess any original health data/individually identifiable health information.
2. The Participant is the repository of the original health data and therefore is the only entity that has the ability to validate the data with their source system.
3. Therefore, the responsibility for ensuring that individually identifiable health information is accurate, complete, and up-to-date falls to Participants and patients.
4. LaHIE has developed policies and procedures to detect, prevent, and mitigate any unauthorized changes to, or deletions of, individually identifiable health information, and has ensured that the process outlined is not unwieldy or inaccessible.
5. Participants, i.e. covered entities, should take reasonable steps to ensure that individually identifiable health information is complete, accurate, and up-to-date to the extent necessary for the Participant's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner. The completeness and accuracy of an individual's health information may affect, among other things, the quality of care that the individual receives, medical decisions, and health outcomes.
6. Participants participating in LaHIE have the responsibility to update or correct individually identifiable health information and to provide timely notice of these changes to others with whom the underlying information has been shared.
7. Participants should develop processes to detect, prevent, and mitigate any unauthorized changes to, or deletions of, individually identifiable health information.
8. LaHIE has developed policies and procedures describing its patient matching approach which ensures that patients are correctly matched with the data that is exchanged about them. These policies also include the accuracy threshold achieved.

LOUISIANA HEALTH CARE QUALITY FORUM

APPROVAL:

A handwritten signature in cursive script that reads "Cindy Munn". The signature is written in black ink and is positioned above a horizontal line.

---

Cindy Munn  
Executive Director  
Louisiana Health Care Quality Forum

## LOUISIANA HEALTH CARE QUALITY FORUM

<b>POLICY:</b> LaHIE Training Policy	<b>EFFECTIVE:</b> 10-01-2011
<b>DEPARTMENT:</b> LaHIE/LHCQF	<b>REVISED:</b>

### PURPOSE

To outline the process used by LaHIE and its Participants in the training of Participants and its Authorized Users.

### PROCESS

#### 1. General Purpose of Training:

- a. The general purpose of the LaHIE training is to assure that in building and operating LaHIE, the focus is maintained on the welfare, safety and concerns of the patients.
- b. All users must be very aware of patient privacy and confidentiality concerns along with being thoroughly trained in the appropriate use of LaHIE.
- c. LaHIE only allows individuals who are trained as part of the LaHIE training program to qualify as Authorized Users to access clinical data through LaHIE or even for the limited purpose of entering status and/or demographic information into LaHIE.
- d. Participating organizations are responsible for training all of its Authorized Users on compliance with applicable HIPAA regulations, privacy laws and rules and the Participant's privacy and security policies.

#### 2. Training Program:

- a. The Health IT Director or designee shall develop and maintain the training materials for usage of LaHIE.
- b. A train-the-trainer model is used with each Participant as part of the Onboarding Process. Each Participant shall determine those individuals designated as the "super users" or training program administrator for training purposes.
- c. Each Participant shall coordinate the training of designated individuals and for implementing the training.
- d. Each Participant will be responsible for assuring that all individuals that are designated as Authorized Users have the proper authorization and followed the Participant's protocol for Authorized Users access.

#### 3. Training of Authorized Users:

- a. As noted above, each Participant will designate their "super users" who will be responsible for deploying training for all of its Authorized Users.
- b. LaHIE staff and support personnel will offer assistance for this training on an as needed basis.
- c. Each Participant shall maintain the documentation of who has been designated as an Authorized User and their training.

LOUISIANA HEALTH CARE QUALITY FORUM

APPROVAL:

A handwritten signature in cursive script, appearing to read "Cindy Munn", is written over a horizontal line.

Cindy Munn  
Executive Director  
Louisiana Health Care Quality Forum

## LOUISIANA HEALTH CARE QUALITY FORUM

<b>POLICY: Notice of Privacy Practices</b>	<b>EFFECTIVE: 10-01-2011</b>
<b>DEPARTMENT: LaHIE</b>	<b>REVISED:</b>

### PURPOSE

To ensure each Participant has developed and maintained a notice of privacy practices (the Notice).

### PROCESS

1. Each Participant shall develop and maintain a notice of privacy practices (the Notice). The Notice must describe the uses and disclosures of protected health information contemplated through the Participant's participation in the Health Information Exchange (LaHIE).
2. The Notice shall meet the content requirements set forth under the HIPAA Privacy Rule (45.C.F.R. § 164.520(b)) and comply with applicable laws and regulations.
3. Participants shall individually determine whether their current Notice requires amendment to reflect their contemplated uses and disclosure of protected health information through the exchange. LaHIE may provide sample language, such as noted below, for Participants upon their request:
  - a. *We may make your protected health information available electronically through an electronic health information exchange to other health care providers that request your information for their treatment and business operations. Participation in an electronic health information exchange also lets us see their information about you for our treatment and business operations.*
4. Each Participant shall have its own policies and procedures governing distribution of the Notice to individuals, and, where applicable, acknowledgement of receipt by the individual (see 45 C.F.R. § 164.520(c)(2)(ii)), which policies and procedures shall comply with applicable laws and regulations.
5. Participants may choose a more proactive Notice distribution or patient awareness process than provided herein and may include more detail in their Notice.

### APPROVAL:



Cindy Munn  
Executive Director  
Louisiana Health Care Quality Forum

## LOUISIANA HEALTH CARE QUALITY FORUM

<b>POLICY: Openness and Transparency Policy for Individually Identifiable Health Information</b>	<b>EFFECTIVE: 10-01-2011</b>
<b>DEPARTMENT: LaHIE</b>	<b>REVISED:</b>

### PURPOSE

To ensure an openness and transparency about policies, procedures, and technologies that directly affects individuals and/or their individually identifiable health information.

### PROCESS

1. Participating organizations, as required by the HIPAA Privacy Rule, must provide a notice of its privacy practices (NPP) to patients, with certain exceptions. This notice of privacy practice should describe how PHI is collected, how it is used, and to whom and for what reason(s) it is disclosed, including the disclosure to a health information exchange. The notice should be:
  - a. Simple, understandable, and at an appropriate literacy level.
  - b. Highlight, through layering or other techniques the disclosures and uses that are most relevant (for example, the notice of privacy practice could have a summary sheet followed by a description of actual use and disclosure practices).
  - c. Adhere to obligations for use of appropriate language(s) and accessibility to people with disabilities.
2. LaHIE has no direct or indirect contact with patients, and thus requires that the duty of providing this notice belong to participating organizations.
3. Individuals should be able to understand what individually identifiable health information exists about them, how that individually identifiable health information is collected, used, and disclosed and whether and how they can exercise choice over such collections, uses, and disclosures.
4. Persons and entities, that participate in LaHIE for the purpose of electronic exchange of individually identifiable health information, should provide reasonable opportunities for individuals to review who has accessed their individually identifiable health information or to whom it has been disclosed, in a readable form and format.
5. Notice of policies, procedures, and technology-- including what information will be provided under what circumstances -- should be timely and, wherever possible, made in advance of the collection, use, and/or disclosure of individually identifiable health information.
6. Policies and procedures developed are consistent with the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information and should be communicated in a manner that is appropriate and understandable to individuals.
7. LaHIE considers PHI to be information that identifies a patient, provided to a participating organization in the Exchange, and can include and includes any part of an individual's medical record or payment history.
8. LaHIE mirrors the definition of protected health information as defined by the Health Insurance Portability and Accountability Act (HIPAA) Standards for Privacy of Individually Identifiable

## LOUISIANA HEALTH CARE QUALITY FORUM

Health Information, 45 C.F.R. Part 160 and Part 164, Subpart E, and the HIPAA Security Standards, 45 C.F.R. Part 160 and Part 164, Subpart C, both as amended from time to time.

9. As a conduit for the exchange of information among Participants, LaHIE does not dictate the type of PHI the Participants collect and share with LaHIE. LaHIE's hybrid infrastructure model will store a minimum amount of health data centrally, primarily facilitating the secure transfer of health data among Participants that store the health data at their disparate locations. LaHIE will enable the exchange of data stored in existing provider networks while maintaining an option to store data centrally (e.g., smaller provider groups without their own database or network; or public health surveillance databases).
10. As part of their policies, Participants must ensure that patients fully understand the nature of the information exchange, and a public relations effort may be required. At a minimum, these topics should be included in the NPP that each patient receives.
  - a. Explain why Participants collect PHI.
  - b. Describing the privacy practices and security safeguards for controlling PHI.
  - c. Disclosing standards, guidelines, regulations and applicable laws regarding PHI.
  - d. Disclosing who has access to PHI and why.
  - e. Providing processes for patient redress.
  - f. Identifying a primary point of contact and/or responsible party for PHI.
  - g. Informing patients of their rights under the privacy policy.
  - h. Providing patient options regarding the collection, use and disclosure of their PHI.

### APPROVAL:



---

Cindy Munn  
Executive Director  
Louisiana Health Care Quality Forum

## LOUISIANA HEALTH CARE QUALITY FORUM

<b>POLICY: Participation Requirements for LaHIE</b>	<b>EFFECTIVE: 10-01-2011</b>
<b>DEPARTMENT: LaHIE</b>	<b>REVISED:</b>

### PURPOSE

To provide guidelines defining the mandatory participation requirements as it relates to the Louisiana Health Information Exchange (LaHIE) provided by the Louisiana Health Care Quality Forum and to outline the process used to onboard Participants onto LaHIE.

### PROCESS

1. Prior to accessing or making clinical data accessible through LaHIE, each Participant must sign:
  - a. The Participation Agreement
  - b. The Business Associates Agreement
2. The Health IT Director or his/her designee is responsible for assuring that each Participant has executed a Participation Agreement prior to participating in the Exchange and/or exchanging Data.
3. As part of the onboarding process, the Participant will provide LaHIE with:
  - a. All the necessary contact information, i.e. Privacy/Security Officer, IT contact, Participation Agreement contact, etc.
  - b. Completed Readiness Questionnaire
  - c. Ensure that all Authorized Users have been properly assigned and documentation acquired.
4. Each Participant will provide system support services necessary for activities related to sharing and viewing data using LaHIE, and for maintaining hardware used in connection with LaHIE.
5. Each Participant is responsible for:
  - a. Maintaining internet connectivity and for the performance of LaHIE as limited by that connectivity.
  - b. Cooperating with LaHIE's staff or support personnel in troubleshooting any difficulties experienced by Authorized Users with respect to access and performance of LaHIE.
  - c. Cooperating with LaHIE and its vendors in testing and implementing the system and any upgrades to LaHIE.
6. Participants that contribute Data to LaHIE are responsible for:
  - a. Monitoring Data Exchanges from its systems to LaHIE's Clinical Data Repository and solving any problems that may arise with respect to such Data Exchanges, ensuring accurate and complete loading of clinical Data from its legacy systems to the Clinical Data Repository. The Participant must notify LaHIE of any problems in the regular Data Exchange to the Clinical Data Repository.
  - b. Ensuring that processes are in place so that the impact on the Clinical Data Repository and LaHIE of any changes to the legacy systems or operating environment are evaluated and tested, as necessary. The Participant must notify LaHIE in advance of any system changes that will require an update to the Clinical Data Repository so that LaHIE can participate in modification and/or testing procedures.
  - c. Monitoring the VPN connectivity and coordinating with LaHIE support services in accordance with the escalation process developed by the Health IT Director or his/her designee as necessary to troubleshoot and resolve any problems or issues.

LOUISIANA HEALTH CARE QUALITY FORUM

APPROVAL:

A handwritten signature in cursive script, appearing to read "Cindy Munn", is written over a solid horizontal line.

Cindy Munn  
Executive Director  
Louisiana Health Care Quality Forum

## LOUISIANA HEALTH CARE QUALITY FORUM

<b>POLICY: Physical security of hardware, data, media and equipment</b>	<b>EFFECTIVE: 10-01-2011</b>
<b>DEPARTMENT: LHCQF; LaHIE</b>	<b>REVISED:</b>

### PURPOSE

To facilitate compliance with all applicable laws and regulations regarding the system security, including, at a minimum (a) meeting the standards established by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) pertaining to system security and workstation security and (b) complying with the security provisions of this Policy Manual with respect to the hardware and systems used by the Louisiana Health Care Quality Forum (LHCQF) and in connection with the Exchange (LaHIE).

### RESPONSIBILITY

LHCQF's Health IT Director or his/her designee shall act as the Security Officer and ensure that LHCQF/LaHIE complies with all applicable laws and regulations regarding the system security and physical security of the hardware, data, media and equipment utilized by the Louisiana Health Care Quality Forum and LaHIE.

Participants of LaHIE shall comply with all applicable laws and regulations regarding system security, including at a minimum, (a) meeting the standards established by HIPAA pertaining to system security and workstation security and (b) maintaining the security of the workstations through which their Authorized Users access LaHIE.

LHCQF's Health IT Director or his/her designee shall ensure that the Exchange's (LaHIE's) technology vendor maintains the security of the hardware located in the vendor's data center (the "Data Center") as well as the hardware maintained by LHCQF staff, i.e. laptops.

### PROCESS

1. LaHIE, Participants and all vendors will comply with, the following system security standards:
  - a. To protect the confidentiality, integrity and availability of LaHIE by taking the reasonable steps to protect hardware used in connection with LaHIE, as well as the facilities in which it is located, from unauthorized physical access, tampering and theft.
  - b. To physically locate hardware used in connection with LaHIE in locations where physical access can be controlled in order to minimize the risk of unauthorized access.
  - c. To take reasonable steps to ensure that the perimeter of facilities containing hardware used in connection with LaHIE is physically sound, the external walls are properly constructed and the external doors have the appropriate protections against unauthorized access.
  - d. To prevent against unauthorized access to the facilities at which hardware used in connection with LaHIE is located by ensuring that doors and windows of all facilities are locked when unattended and that external protections, such as window guards or bars, are installed on all windows at ground level and any other windows as reasonably necessary to prevent unauthorized entry.
  - e. To establish and document detailed rules to determine which workforce members are granted physical access rights to specific areas where hardware used in connection with LaHIE is maintained and to provide such physical access rights to the work area only to

## LOUISIANA HEALTH CARE QUALITY FORUM

workforce members having a need for access to such an area in order to complete job responsibilities.

### 2. Data Center Security Standards

- a. To use the following controls at all delivery and loading areas to prevent unauthorized access to its facilities:
    - i. Restrict access to a holding area from outside building to identified and authorized workforce members
    - ii. Design the holding area so supplies can be unloaded without the delivery staff gaining access to other areas of the building.
    - iii. Secure the external doors of the holding area when the internal door of the area is open.
  - b. To take reasonable steps to ensure that the level of protection provided for LaHIE, as well as the facilities in which they are housed, is commensurate with that of the identified threats and risks to the security of LaHIE and its facilities.
3. Periodic risk analysis will be performed by LHCQF's Health IT Director or his/her designee in order to assess the level of physical access risk and adjust procedures accordingly.
  4. LHCQF's staff laptops will not contain unencrypted PHI on the hard drive.

### APPROVAL:



---

Cindy Muniz  
Executive Director  
Louisiana Health Care Quality Forum

## LOUISIANA HEALTH CARE QUALITY FORUM

<b>POLICY: Sanction Policy</b>	<b>EFFECTIVE: 10-01-2012</b>
<b>DEPARTMENT: LHCQF; LaHIE</b>	<b>REVISED:</b>

### PURPOSE

To establish appropriate sanctions for full-time, part-time LHCQF employees or support personnel, i.e. trainees, volunteers, contractors and temporary employees, who fail to comply with the privacy or security policies of LHCQF as well as state and federal regulations such as HIPAA Security Rule, Security Management Process standard (164.308(a)(1)).

### PROCESS

1. **Violation of LHCQF privacy or security policies and procedures.** Failure to comply with the LHCQF privacy or security policies or procedures will result in disciplinary action against the individual committing the violation.
  - a. LHCQF privacy and security policies and procedures will be enforced consistently across the organization.
  - b. Sanctions that are imposed as a result of a violation of a LHCQF privacy or security policy or procedure will be imposed consistently across the organization.
  - c. The following types of conduct on the part of a member of LHCQF's workforce will result in disciplinary action against the individual engaging in the conduct:
    - i. Accessing PHI out of curiosity or for any purpose outside of treatment, payment or health care operations.
    - ii. Discussing PHI in a public area or outside of LHCQF.
    - iii. Failing to logoff or leaving a computer monitor on and unsecured when PHI is being displayed.
    - iv. Using PHI for personal reasons (such as developing a personal relationship with the patient) rather than for legitimate and authorized business reasons.
    - v. Copying or compiling PHI with the intent to sell or use the PHI for personal or financial gain.
    - vi. "Hacking" into or otherwise attempting to gain unauthorized access into LHCQF computer systems, network devices and/or applications.
    - vii. Failing to follow procedures to ensure secure transmissions of PHI across an open network.
    - viii. Downloading unauthorized software to LHCQF systems, including laptops, PDAs, phones, iPads, and USB storage devices.
2. **Disciplinary action that may be taken.**
  - a. Disciplinary action will be recommended by management and Human Resources contractor services, in consultation with the Privacy or Security Officer or Legal Counsel, as appropriate. It will be determined on a case by case basis, taking into consideration the specific circumstances and severity of the violations; and

## LOUISIANA HEALTH CARE QUALITY FORUM

- b. May be up to and including termination of employment, or of the business relationship as appropriate.
  - c. Sanctions that may be imposed include, but are not limited to:
    - i. Verbal reprimand by the employee's immediate supervisor, with summary documentation to the employee's personnel file;
    - ii. A written warning letter to the employee's personnel file;
    - iii. Administrative leave without pay;
    - iv. Attendance and successful completion of additional training;
    - v. Reimbursement of expenses incurred by LHCQF to resolve this matter; or
    - vi. Immediate termination of employment.
3. **Violations of state or federal confidentiality laws and regulations.** Workforce members who knowingly and willfully violate state or federal law for improper use or disclosure of an individual's information are subject to criminal investigation and prosecution or civil monetary penalties.
4. **Duty to report.** Any workforce member who observes or becomes aware of or suspects a wrongful use or disclosure of PHI maintained by LHCQF is required to report his or her suspicion or the wrongful use or disclosure as soon as possible to his/her supervisor or LHCQF Privacy Officer. Workforce members who become aware of security breaches must notify the Security Officer of the breach.
  - a. A workforce member who makes a report of a suspected or actual improper use or disclosure in good faith will not be retaliated against for making the report.
  - b. A workforce member who fails to report either a suspected or actual violation will have violated this Policy, and may be subject to disciplinary action, up to and including termination.
5. **No retaliation for good faith reports.** LHCQF will not retaliate against a member of its workforce who acts in good faith believing the practice he or she reports is unlawful or violates LHCQF policy. Any employee that believes that he or she has been subject to retaliation should immediately notify LHCQF Human Resources contractor.

### APPROVAL:



---

Cindy Munn  
Executive Director  
Louisiana Health Care Quality Forum

## LOUISIANA HEALTH CARE QUALITY FORUM

<b>POLICY:</b> Security Breach Response Protocol	<b>EFFECTIVE:</b> 10-01-2011
<b>DEPARTMENT:</b> LHCQF; LaHIE	<b>REVISED:</b>

### PURPOSE

To establish a Security Breach Response Protocol ("Protocol") for a LHCQF employee to use as a resource upon becoming aware of an actual or possible security incident. The Protocol describes a recommended process for responding to such incidents, but recognizes that an appropriate type of response will depend on the specific facts of each incident and applicable federal and state laws.

### RESPONSIBILITY

All LHCQF employees involved in the access, use, release or disclosure of electronic protected health information ("ePHI").

### DEFINITIONS

1. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of ePHI or interference with systems operations in an information system.
  - a. An *attempted* or *unsuccessful* security incident means that there was no actual access, use, disclosure, etc. Examples of an attempted or unsuccessful security incident include, but are not limited to:
    - i. Pings on a firewall;
    - ii. Malware;
    - iii. Denial-of-service attacks that do not result in a server taken off-line;
    - iv. Port scans; and
    - v. Attempts to log on to a system, application or database with an invalid password or user name.
  - b. A *successful* security incident means that there was actual unauthorized access, use, disclosure, etc. Examples of a successful security incident include, but are not limited to:
    - i. ePHI sent to an unintended recipient;
    - ii. An employee using another user's identification to access ePHI;
    - iii. Unauthorized access by an employee; and
    - iv. Failure to comply with LHCQF's privacy and security policies and procedures.

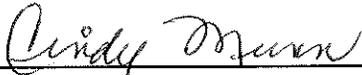
## LOUISIANA HEALTH CARE QUALITY FORUM

2. A security breach is a successful security incident that has been assessed as having a high or severe threat of harm, vulnerability or impact to LHCQF or LHCQF's customers. The Executive Director and/or the Health IT Director in concert with Legal Counsel will assess the security incident to determine the risk level.

### PROCESS

1. LHCQF has developed a Security Breach Response Protocol (see attached) that may be used as a resource to guide employees that become aware of a possible or actual successful security incident involving the ePHI of LHCQF or of a LHCQF customer.
2. Attempted or unsuccessful security incidents should be reported as soon as possible to LHCQF's Health IT Director or his/her designee.
3. Successful security incidents should be reported immediately to LHCQF's Health IT Director or his/her designee.

### APPROVAL:



---

Cindy Munn  
Executive Director  
Louisiana Health Care Quality Forum



LOUISIANA  
HEALTH CARE  
QUALITY FORUM

WORKING TOGETHER FOR A HEALTHIER STATE

# **Security Breach Response Protocol**

***Procedures for Responding to a Security Breach Involving  
Electronic Protected Health Information***

**TABLE OF CONTENTS**

	Page
<u>Introductions</u> .....	3
<u>Definitions</u>	
Protected Health Information .....	3
Security Incident .....	3
Security Breach .....	4
<u>Security Incident Reporting (Low-Medium Risk)</u>	
Security Incident (Low Risk).....	4
Security Incident (Low-Medium Risk).....	4
<u>Security Breach Response Team</u>	
Team Composition .....	5
Team Objectives .....	5
<u>Response to a Security Breach</u>	
Activation of the Team .....	5
Determination of the Team .....	5
Communications and Notifications .....	6
Recording the Incident .....	6
Ongoing Security Response Activities .....	6
<u>Post-Incident Actions</u>	
Post-Incident Actions .....	6
<u>Appendix</u>	
Risk Assessment Process .....	7

## LOUISIANA HEALTH CARE QUALITY FORUM

### INTRODUCTION

The purpose of this Security Breach Response Protocol ("Protocol") is to establish formal documented procedures to be followed when LHCQF becomes aware of instances of unauthorized access to or disclosure of, patients' protected health information ("PHI"), in accordance with applicable state and federal laws and LHCQF's policies.

This Protocol describes a recommended process for responding to such incidents, the conditions whereby this process is invoked, the resources required, and the course of recommended action. The primary emphasis of activities described within this Protocol is the return to a normalized (secure) state as quickly as possible, while minimizing the impact to LHCQF, LHCQF's customers and to the individuals/patients. However the appropriate type of response will depend on the specific facts of each PHI disclosure incident and applicable federal and state laws, and thus the process recommended by this Protocol may have to be revised accordingly.

This Protocol establishes the Security Breach Response Team, which shall have the responsibility for the actions contained herein.

### DEFINITIONS

1. **Protected Health Information (PHI):** as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), protected health information<sup>1</sup> is defined as health information, including demographic information collected from an individual, and:
  - (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
  - (2) Relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
    - (i) that identifies the individual; or
    - (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
2. **Security Incident:** a Security Incident<sup>2</sup>, as defined by HIPAA, means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. A Security Incident poses a threat to LHCQF's or LHCQF's customers' physical environment or information systems. Each Security Incident will be evaluated and assessed a risk score based on the threat, vulnerability and impact of the Incident (See Appendix).

Examples of a Security Incident assessed as Low (score of 4 or less) may include, but are not limited to:

- a. Pings on a firewall;
- b. Malware;
- c. Denial-of-service attacks that do not result in a server taken off-line;

---

<sup>1</sup> 45 C.F.R. 160.103

<sup>2</sup> 45 C.F.R. 164.304

## LOUISIANA HEALTH CARE QUALITY FORUM

- d. Port scans;
- e. Attempts to log on to a system or application, or enter a database with an invalid password or user name.

Examples of a Security Incident assessed as Medium (score of 5-6) may include, but are not limited to:

- a. PHI sent to an unintended recipient;
- b. An employee using another user's identification;
- c. Unauthorized access to PHI by an employee;
- d. Failure to comply with LHCQF's privacy and security policies and procedures.

- 3. Security Breach:** A Security Incident assessed as High (score of 7-8) or Severe (score of 9), will be considered a Security Breach, requiring activation of this Protocol.

Examples of a Security Breach may include, but are not limited to:

- a. Intentional, unauthorized access to LHCQF's customers' data with the intent to sell, transfer, use for commercial advantage, personal gain, or malicious harm;
- b. Theft or loss of portable media (such as unencrypted laptops or USB sticks) containing electronic PHI;
- c. Law enforcement investigations that involve LHCQF's information or personnel that may impact LHCQF's or LHCQF's customers' information, systems, facilities or workforce;
- d. A Security Incident that, although unintentional, has a substantial risk of harm to a high number of individuals.

### PROCESS

**1. Security Incident Reporting (LOW-MEDIUM RISK):**

- a. Security Incident (Low Risk): Unsuccessful Security Incidents, such as attempts to access, misuse, disclose, modify or destroy information or physical assets shall be logged and tracked by LHCQF in accordance with LHCQF's policies and procedures. The Health IT Director or his/her designee shall be responsible for reviewing such logs and taking appropriate actions.
- b. Security Incident (Low – Medium Risk): Any employee, data owner or customer who believes that a successful Security Incident has occurred, shall immediately notify the Health IT Director upon becoming aware of such Security Incident.

- 2.** The Executive Director or his/her designee will conduct an investigation, coordinate the investigation with stakeholders, as appropriate to the incident, including, but not limited to: Information Security, customers and business associates, Human Resources, and others, as appropriate. The Executive Director or his/her designee shall maintain written documentation of the Security Incident, such as a description of the incident, root cause of the incident, remediation actions taken, and corrective measures applied.

If, during the investigation, the Executive Director determines that a Security Breach has occurred, he/she will immediately activate the Security Breach Response Team.

## LOUISIANA HEALTH CARE QUALITY FORUM

### 3. Security Breach Response Team:

- a. Security Breach Response Team (“Team”) Composition – The Executive Director, or his/her designee, will be responsible for activating the Security Breach Response Team. Depending on the circumstances of the Security Breach, the Team will be comprised of appropriate representatives from the organization and/or customer affected.
- b. Team Objectives – The Team will take all commercially reasonable steps to minimize the potential negative impact of the Security Breach and restore services to a normalized and secure state of operations as soon as possible. In addition, the Team will:
  - i. Coordinate and oversee the response to a Security Breach in accordance with the requirements of state and federal laws and LHCQF’s policies;
  - ii. Where appropriate or as required by law, inform the affected individuals and third parties of action that is recommended or required on their behalf;
  - iii. Provide clear and timely communication to all interested parties.
  - iv. Conduct a post-Security Breach review;
  - v. Ensure appropriate actions are taken to prevent a recurrence;
  - vi. Establish, maintain and document periodic Security Breach Response Protocol testing;
  - vii. Review the Security Breach Response procedures at least annually and update as necessary.

### 4. Response to a Security Breach

- a. Activation of the Team - The Executive Director or his/her designee shall be responsible for activating the Team and providing an initial report to the Team and Executive Management.

*Note: The following procedures may repeat or be concurrent depending upon the incident.*

- b. Determination of the Risk - The Team will assess the risk to LHCQF or LHCQF’s customer posed by the Security Breach by developing a risk assessment scoring tool (See Appendix) that is based on:
  - o Threat (probability)
    - Malicious – intentional, targeted at LHCQF
    - Inadvertent – untargeted threat
  - o Impact (criticality)
    - Determine the potential damage and business impact of the incident
    - Determine if the incident has or will affect businesses or resources outside of the LHCQF network
  - o Vulnerability (exposure)

## LOUISIANA HEALTH CARE QUALITY FORUM

- Determine if the incident is localized in nature or company wide
- c. Communications and Notifications - The Executive Director will coordinate all internal and external communications and notifications as appropriate to the circumstances, including, but not limited to:
  - State and/or federal law enforcement
  - Regulators
  - Media
  - Customers, vendors and clients
  - Employees
- In addition:
  - Only the designated spokesperson, i.e., the Executive Director, or his/her designee, shall speak directly with the media;
  - All notifications will be documented, including date and time of notification, who was notified and who made the notification;
  - All communications pertaining to a Security Breach must be on a confidential, need-to-know basis;
  - The Executive Director shall monitor and communicate ongoing progress of the Security Breach investigation.
- d. Recording the Incident – The Executive Director or his/her designee shall securely maintain all documentation relating to the Security Breach, including, but not limited to: a log of all activities and events in response to the Security Breach.
- e. Ongoing Security Response Activities – during the course of the investigation, the Executive Director, or his/her designee, working with the Team may:
  - i. Determine what additional parties need to be involved in the issue resolution;
  - ii. Transfer some or all responsibility to the LHCQF Security Breach Response Team (SBRT) upon completion of the risk assessment. The IRT is under the direction of the Executive Director or his/her designee;
  - iii. Identify and contact additional functional areas and/or individuals, as needed to respond.
- 5. Post-incident actions - The following actions will be initiated by the Executive Director and require involvement of the Team members or individuals, as appropriate:
  - a. Meet with the Team and other appropriate individuals to assess the actual impact of the Security Breach;
  - b. Lead efforts to determine root cause, if not already discovered;
  - c. Designate responsibility for any follow-up security remediation activities to the appropriate business area/service line;
  - d. Ensure that appropriate Security Breach notification is conducted to covered entities where LHCQF is the business associate;
  - e. Ensure each functional area has maintained chain of custody for collected evidence;

## LOUISIANA HEALTH CARE QUALITY FORUM

- f. Identify and recommend the appropriate retroactive and prospective corrective actions to the Executive Committee;
- g. Communicate final reporting to Executive Management, and others, as appropriate;
- h. Declare the Security Breach response as completed;
- i. Conduct "Lessons Learned" session(s);
- j. Review/revise the Team procedures if needed;
- k. Provide final report to Executive Management, the Executive Committee, and the Board of Directors.

**LOUISIANA HEALTH CARE QUALITY FORUM**

**APPENDIX**

**SECURITY RISK ASSESSMENT PROCESS**

The Team will assess risk based on: (a) protecting the safety and personal well-being of the LHCQF workforce and others; and (b) protecting the confidentiality, integrity, and availability of the LHCQF information and information assets.

Risk will be assessed using the following three factors:

1. Threat – the likelihood (or actual event) that puts personnel or information resources at risk of harm, loss of confidentiality, integrity, or availability, or corruption of data;
2. Vulnerability – the exposure of personnel or information to potential threats;
3. Impact – the impact of the loss of information or personnel. This can be quantified in financial terms or qualified by importance to business operations (i.e., high, medium, or low.)

Threat	Vulnerability	Impact
<ul style="list-style-type: none"> <li>• An actual security breach has occurred or the probability of occurrence is extremely high (over 70%)</li> <li>• The nature of the threat is malicious in nature and cannot be effectively managed with existing controls</li> <li>• The threat is demonstrable and pervasive in the physical or computing environments</li> </ul>	<ul style="list-style-type: none"> <li>• Exposure to a particular threat is extremely high</li> <li>• Large volume of un-patched systems</li> <li>• Exposures that are easily gained</li> <li>• Large amount of data available in a particular facility</li> </ul>	<ul style="list-style-type: none"> <li>• Situation where personnel are at serious risk of harm</li> <li>• Financial impact of loss of data or system assets is significant</li> <li>• Security incident may cause significant embarrassment to LHCQF, LHCQF’s customers, or individuals through media attention</li> <li>• Mitigation of vulnerability would be a serious impact to business operations</li> <li>• Significant operational impact resulting in the impact of critical business recovery time objectives</li> <li>• Estimated impact: over \$500,000</li> </ul>

LOUISIANA HEALTH CARE QUALITY FORUM

<b>Medium</b>	<ul style="list-style-type: none"> <li>• The probability of an actual security breach occurring is likely (30-70%)</li> <li>• The threat can be managed somewhat effectively with existing controls</li> <li>• The threat has been demonstrated to be effective against vulnerable systems – low number of incidents reported</li> </ul>	<ul style="list-style-type: none"> <li>• Exposure to a particular threat is moderate in scope</li> <li>• Measurable amount of information systems that are exposed</li> <li>• Access to systems, data, or personnel is moderately difficult to gain</li> </ul>	<ul style="list-style-type: none"> <li>• Financial impact of loss of data or system assets is measurable but not significant</li> <li>• Risk is not posed to PHI or other information assets of a confidential nature</li> <li>• Mitigation of vulnerability is not a significant impact to business operations</li> <li>• An incident that results in or is likely to result in significant impact to operations, including exceeding critical business unit maximum allowable delays</li> <li>• Estimated impact: Between \$50,000-\$500,000</li> </ul>
	<ul style="list-style-type: none"> <li>• The probability of an actual security breach occurring is low (less than 30%)</li> <li>• The threat can be managed effectively with existing controls</li> <li>• The threat is conceptual or perceived – no known incidents reported</li> </ul>	<ul style="list-style-type: none"> <li>• Exposure to a particular threat is low</li> <li>• Negligible amount of information systems that are exposed</li> <li>• Access to systems, data, or personnel is difficult to gain</li> </ul>	<ul style="list-style-type: none"> <li>• Financial impact of loss of data or system assets is not significant</li> <li>• Risk is not posed to sensitive information assets</li> <li>• Mitigation of vulnerability does not impact business operations</li> <li>• Minor data communications interruption</li> <li>• Estimated impact: Under \$50,000</li> </ul>

The Team must evaluate the security event using the above criteria as a guideline to determine the appropriate risk for each factor. A high-level risk posed against a low-level criticality may be determined to be of low-medium overall risk to LHCQF.

The following procedure for evaluating the security event shall be used to determine if the event should be classified as a Security Incident or a Security Breach, and to drive the appropriate levels of response.

LOUISIANA HEALTH CARE QUALITY FORUM

For each category (Threat, Vulnerability, Impact), the risk-level is scored as follows:

- High = 3 points
- Medium = 2 points
- Low = 1 point

EXAMPLE

	Threat	Vulnerability	Criticality	TOTAL
High	3			3
Medium		2	2	4
Low				0
TOTAL	3	2	2	7

Once each area is scored, total the values across the table, then down, to gain the Overall Risk Rating.

Each area will be assigned a score and the total will allow for ranking the risk:

- SEVERE (or Critical if non-system related): 9 points
- HIGH: 7 - 8 points
- MEDIUM: 5 - 6 points
- LOW: 3 - 4 points

## LOUISIANA HEALTH CARE QUALITY FORUM

<b>POLICY:</b> User Permissions Policy	<b>EFFECTIVE:</b> 10-01-2011
<b>DEPARTMENT:</b> LaHIE	<b>REVISED:</b>

### PURPOSE

Patient privacy policies have been enabled by the Orion Health platform to control access to patients protected health information. This access is based on the following:

- The user's relationship with the patient
- The patient's opt-in status

### PROCESS

#### 1. Access descriptions:

- No Access – the patient's name will not be visible to the user in a work list or list of search results.
- Locked – the patient's name (demographic information) will be visible in a list of search results, but cannot be selected.
- Privacy sealed – the patient's name will be visible and can be selected, but a reason for access will be required before the patient can be placed in context and their medical details viewed.
- Full Access – clinical users have unrestricted access to clinical data/documents in the patient's medical record as they have a valid relationship with the patient and the patient has "opted-in", i.e. chosen to have their information available in the HIE.

#### 2. Providing an access reason is referred to as "Opening the privacy seal".

- Once this has been done, the user will be able to access that patient's record for a limited period of time without having to reapply the reason.
- This time is configurable (as a single global variable for the whole solution) and the default is 12 hours. If the clinical user ends his/her Portal session, all open privacy seal access is ended and he or she will need to re-supply the reason for viewing the restricted information.
- List of reasons for when the user "breaks the glass" and a comment field for free text for each.

#### 3. List of reasons for when the user 'breaks the glass':

- Direct patient care - clinician or primary care provider
- Direct patient care – consultant
- Direct patient care – emergency
- Direct patient care-clinician requested

#### 4. Provider-patient relationships are established via HL7 ADT messages from the participants EHR/registration systems. These include admitting physician, attending physician, primary care physician, referring physician.

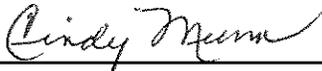
## LOUISIANA HEALTH CARE QUALITY FORUM

### 5. Data access rules:

- Sensitive patient information is applied based on specific blocked codes. This applies to:
  - Lab/Micro results (LOINC)
  - Medications (RxNorm)
  - Problems (ICD-9-CM)
  - Encounters (Diagnosis ICD-9-CM Code)
  - Procedures (CPT codes)
- The rules around who can see sensitive data:
  - Level 1 Provider – Privacy Sealed Access only
  - All other users – No access.

6. Each Participant and LaHIE shall have an **authorization process** in place to ensure users have access to only those applications and the protected health information that they are allowed to use or review.

### APPROVAL:



---

Cindy Munn  
Executive Director  
Louisiana Health Care Quality Forum