State of Nevada

Department of Health and Human Services
Division of Health Care Financing and Policy

Implementation Advanced Planning Document

Electronic Health Record
Provider Incentive Payment Program

May 4, 2011

TABLE OF CONTENTS

Tables

Figures

1 Introduction and Overview

The Nevada Division of Health Care Financing and Policy (DHCFP) submits this Implementation Advanced Planning Document (IAPD) to request approval for the completion of the acquisition, design, development, implementation, maintenance, and operation of the Nevada Provider Incentive Program (NPIP). NPIP is for those Nevada eligible hospitals (EHs) and eligible professionals (EPs) (collectively Providers) that have adopted, implemented, or upgraded (AIU) or become meaningful users (MU) of certified electronic health record (EHR) technology.

The goal of NPIP is to provide access to enhanced Medicaid funds to Providers to offset the cost of implementation of certified EHR technology. This funding is designed to promote the adoption of certified EHR technology and ultimately provide improved quality of care for Medicaid beneficiaries and increased cost efficiencies within the Medicaid enterprise.

DHCFP has completed a strategic planning effort that resulted in the submission of the State Medicaid Health Information Technology Plan (SMHP) for approval to the Centers for Medicare and Medicaid Services (CMS) on April 13, 2011. The planning effort was conducted in accordance with the State Planning Advance Planning Document (P-APD) that was approved on February 23, 2010. Specifically, DHCFP conducted planning activities that resulted in the development of an "As-Is" landscape for health information technology (HIT), the development of a vision of the HIT activities through 2014 that resulted in a "To-Be" document, and the creation of a roadmap of steps to move from the "As-Is" to the "To-Be." Furthermore, DHCFP identified the actions necessary to implement an incentive payment program. As part of its planning activities, DHCFP engaged stakeholder organizations and participated in the planning activities for the Statewide Health Information Exchange (Statewide HIE).

As part of the planning process for the NPIP functionality for Provider registration, attestation, payment, and tracking, DHCFP is considering vendor solutions being used in other states. DHCFP has received draft cost proposals from three vendors that provide electronic solutions for the program and has had demonstrations from two of the three vendors. DHCFP intends to follow the State procurement process in procuring a vendor solution. Since the submission of the SMHP, requirements in the State procurement process have caused a change in the proposed timeline. Upon completion of the procurement process, DHCFP expects that testing with CMS' National Level Repository (NLR) will begin in April 2012. It is anticipated that the Nevada Medicaid EHR Incentive Program will begin accepting registrations in June 2012 with the first incentive payments being made in July 2012. If decisions made during the procurement process significantly affect timelines or costs, the changes will be communicated to CMS in an update to this document.

The vendor solution will provide DHCFP with the capability of communicating with the NLR in full compliance with CMS requirements. In addition to the attestation and registration solution, DHCFP also plans to make modifications to the Medicaid Management Information System (MMIS), as necessary, that will allow the MMIS to make payments to Nevada Providers in accordance with the timelines required by CMS. Part of the implementation of this program includes a Provider outreach and education process. Moreover, DHCFP has plans in place to conduct verifications and audits to identify and limit fraud and abuse of the incentive payment program. DHCFP plans to manage NPIP with leadership from

the Information Systems Projects Office that is part of the MMIS/IT Unit with assistance from the Compliance Unit, the Audit Unit, and the Accounting and Budget Unit.

This IAPD sets forth the projected timeline for DHCFP activities and readiness to launch NPIP, outlined in the table below.

Table 1: Remaining Key Action Dates

ACTION	DATE (calendar year)
1. Submission of SMHP and IAPD	Q2 2011
2. Continue provider outreach and education efforts	Q2 2011 thru Q2 2012
3. State procurement process	Q3 2011 thru Q4 2011
4. Implement vendor solution	Q1 2012 thru Q2 2012
5. Testing with the NLR	Q2 2012
6. NPIP ready to accept registrations	Q2 2012
7. MMIS system ready to pay incentives	Q2 2012
8. First incentive payment	Q3 2012

This IAPD also details DHCFP's needs and objectives for this funding, as well as a statement of alternative considerations. DHCFP considered an in-house solution that would have required MMIS modifications and manual processes. DHCFP also considered vendor solutions and participation in a multi-state consortium.

This IAPD document includes a description of the nature and scope of the methods to be used to accomplish the implementation as well as an activity schedule.

The budget that is included with this IAPD considers the costs to implement NPIP and is shown by specific categories of costs that include:

- Procurement or acquisition costs;
- State personnel;
- Contractor services;
- Hardware, software and licensing;
- Equipment and supplies;
- Training and outreach;
- Travel;
- Administrative operations;
- Miscellaneous expenses for the project;

- Estimate of prospective cost distribution to the various State and federal funding sources and the proposed procedures for distributing costs that includes the total planned payment amounts and the calendar year of each planned annual payment amount;
- Security and interface requirements for all State HIT systems; and
- Disaster recovery procedures.

In order to meet the proposed launch date in June 2012, DHCFP is pleased to submit this IAPD, to accompany the previously submitted SMHP, as documentation of its activities to comprehensively plan and implement its future vision as a partner to its Providers and other stakeholders in the adoption of certified EHR technology and the promotion of HIE.

Respectfully submitted by:

Ms. Peggy Martin
Project Manager
Telephone: 775-684-3735
Email: peggy.martin@dhcfp.nv.gov

Mr. Justin Luna
Project Lead
Telephone: 775-684-3734
Email: justin.luna@dhcfp.nv.gov

2 Statement of Needs and Objectives

This section describes DHCFP's purpose and objectives for the program. DHCFP seeks to administer NPIP for its Providers, oversee this program, and pursue initiatives that promote the adoption of certified EHR technology for the promotion of health care quality and the electronic exchange of health information. DHCFP has completed its SMHP that details the current HIT landscape ("As-Is") in the State, the future HIT landscape and Provider adoption plan ("To-Be"), and the roadmap for implementation. The SMHP explains the need for this program, as well as the detailed request for implementation funding from CMS. This document is the request for funding. Specifically, DHCFP seeks funding for the following elements of NPIP:

- Administration: DHCFP plans to administer NPIP in accordance with CMS requirements as detailed in 42 CFR Part 495.
- Oversight: DHCFP plans to collect AIU and MU data from Providers' EHRs and to develop, capture, and audit Provider attestations.
- Promotion: DHCFP will pursue initiatives to encourage the adoption of certified EHR technology to promote health care quality and exchange of health care information.

3 Statement of Alternative Considerations

DHCFP studied multiple alternative solutions for its incentive payment program, including:

- A manual incentive payment system, staffed and operated by State staff;
- An in-house developed automated incentive payment system; and
- Web-based hosted solutions being developed by vendors in the MMIS space and offered as Software as a Service (SaaS) solutions. Designed as adjuncts to the current MMIS, the SaaS solutions require minimal changes to the current MMIS. They offer attestation and tracking capabilities to support AIU and MU, and provide a State Level Repository (SLR) to document and track Providers' use of EHRs. The SLR works in conjunction with and communicates with CMS' NLR in accordance with the published interface specifications.

A comparison of internally developed systems and SaaS solutions is presented in the following table. Important considerations in DHCFP's decision-making process are timeliness, availability of qualified State staff, and expense.

Table 2: Internal Solution v. SaaS Solution

Considerations	Internal Solution/SaaS Solution
The State desires a solution that poses the least risk of schedule delay.	Internal Solution: The required State resources do not have time to develop and implement a solution.
	SaaS Solution: Vendors are devoting significant resources to creating solutions for multiple states.
The State desires a solution that requires the least amount of limited state resources.	Internal Solution: The required State resources will be significant under this scenario (support, maintenance, development, programming, help desk, and project management). The State may struggle to recruit sufficient resources in a timely manner.
	SaaS Solution: The State would require minimal resources for oversight and management of the proposed solution.
The State desires a solution that meets all Nevada-specific requirements.	Internal Solution: An internal solution will be able to meet any Nevada-specific requirements.
	SaaS Solution: Vendor solutions may not meet all Nevada-specific requirements. Furthermore, substantial modifications may be expensive and/or time consuming.
The State desires a solution that conforms to all SMHP requirements.	Internal Solution: An internal solution may require additional manual processes for attestation and verification, but will be able to meet all SMHP requirements.
	SaaS Solution: Vendor solutions include Web-based systems to support MU requirements, incentive payments, and other ARRA HITECH Act requirements. These solutions provide a more automated solution for the attestation and verification processes, thereby requiring fewer State resources.

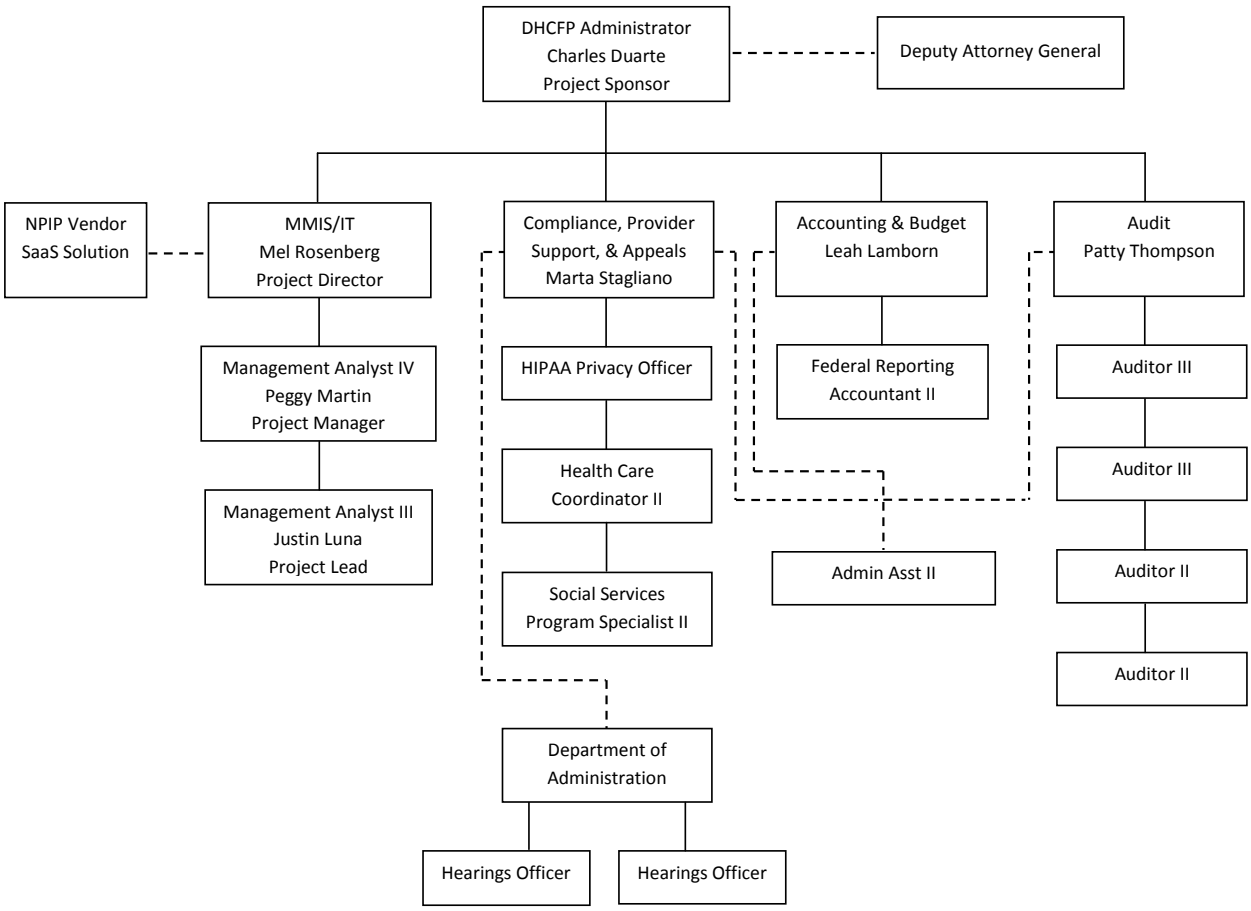
Considerations	Internal Solution/SaaS Solution
The State desires a solution that is flexible, easily modifiable, and maintainable.	Internal Solution: Building applications that are easy to modify and maintain is a challenge and very time consuming. The State may struggle to create an internal solution to meet these objectives while altering a legacy MMIS at the same time.
	SaaS Solution: Vendors state that their solutions can be modified, but have not provided enough information to verify claims of flexibility.
The State desires a solution that provides as much automation as possible for audit functions.	Internal Solution: An internal solution may be able to automate audit functions fully, but design, development, and implementation may take a significant amount of time.
	SaaS Solution: Vendor solutions provide automation of audit functions. The full extent of those automation capabilities is yet to be determined at this point.

Based on a comparison of the above alternatives, the State has chosen to procure a Web-based hosted solution being developed by a vendor in the MMIS space and offered as a SaaS solution as it provides the lowest risk and appears to offer a lower-cost alternative long term.

4 Personnel Resource Statement

DHCFP plans to manage the payment of the incentives using the current organization. Specifically, NPIP will be managed with leadership from the Information Systems Projects Office that is part of the MMIS/IT Unit with assistance from the Compliance Unit, the Audit Unit, and the Accounting and Budget Unit. The DHCFP organization chart for this project is shown below.

Figure 1: NPIP Internal DHCFP Organization Chart



The following table includes current internal staff as well as projected new staff to manage tasks associated with administration of NPIP for years one and two.

Table 3: NPIP Internal DHCFP Staffing Projections for Years One and Two

Position	Organizational Location	% of Full Time Employee	Responsibility	Classification Hourly Rate + 35% benefits factor Estimated Annual Salary Expense
Executive Project Sponsor (Charles Duarte)	DHCFP	10%	Executive administration of the program. Participate in Blue Ribbon Task Force.	Unclassified position $56.04 $15,131.00
HIT Project Director (Mel Rosenberg)	DHCFP	20%	Manage data sharing agreement efforts. Oversight of implementation vendor. Coordinate NHIN efforts.	LG 41 $42.60 $23,004.00
HIT Project Manager (Peggy Martin)	DHCFP	25%	Manage stakeholder meetings. Coordinate HIT Planning and implementation efforts with internal and external stakeholders. Manage certain third party contracts.	LG 39 $38.86 $26,231.00

Position	Organizational Location	% of Full Time Employee	Responsibility	Classification Hourly Rate + 35% benefits factor Estimated Annual Salary Expense
HIT Project Lead (Justin Luna)	DHCFP	100%	Manage the Statewide HIE coordination. Manage certain third-party contracts. SMHP/IAPD preparation and updates. Environmental Scan updates. Provide overall program oversight. Conduct Pre-Payment verification. Coordinate stakeholder communications. Manage policy changes (writing policy). Draft TIR for HIT/HIE initiatives. Coordinate reporting requirements. Develop HIT project Office budget. Prepare CMS quarterly and annual reports for compliance with SMHP and IAPD activities.	LG 37 $35.48 $95,796.00
Project Support Admin Asst. II	DHCFP	100%	Administrative support for EHR Incentive Program. Including Provider support and hearings support.	LG 25 $20.90 $56,430.00
Deputy Attorney General	Attorney General's office	5%	MFCU referrals. Manage the review and revisions of Nevada regulations and policy. Advise on compliance with HIPAA and HITECH. Hearings functions (prepare evidence, respond to pleadings).	Unclassified position $45.80 $6,183.00

Position	Organizational Location	% of Full Time Employee	Responsibility	Classification Hourly Rate + 35% benefits factor Estimated Annual Salary Expense
Chief of Compliance (Marta Stagliano)	DHCFP	10%	Manage Provider support, SURS, HIPAA/Civil Rights, and Hearings Officers relating to incentive program oversight. Manage hearings process.	LG 41 $42.60 $11,502.00
Audit Chief (Patty Thompson)	DHCFP	25%	Manage pre and post payment audits (AIU and MU). Program integrity internal compliance audits (ex. Account and Budget internal controls using desk audit process) Audit and monitor cost allocation plans for Providers.	LG 41 $42.60 $28,755.00
Chief of Accounting and Budget (Leah Lamborn)	DHCFP	5%	Manage CMS Reports	LG 41 $42.60 $5,751.00
Auditor III (new positions)	DHCFP	2 @ 100%	Audit AIU – Year One. Audit Post Payment - Year Two. Audit MU – Year Two. Participate in fair hearings process.	LG 36 $33.91 $183,114.00
Auditor II	DHCFP	2 @ 50%	Audit Post Payment - Year Two. Audit MU – Year Two. Participate in fair hearings process.	LG 34 $30.99 $167,346.00
Federal Reporting Accountant II	DHCFP	5%	Prepare CMS reports.	LG 36 $33.91 $4,578.00
HIPAA Privacy Officer	DHCFP	15%	Participate in HIPAA privacy and security policy development and updates to comply with HITECH	LG 37 $35.48 $13,734.00
Health Care Coordinator II in Compliance	DHCFP	100%	Hearings Officer support.	LG 37 $35.48 $95,796.00

Position	Organizational Location	% of Full Time Employee	Responsibility	Classification Hourly Rate + 35% benefits factor Estimated Annual Salary Expense
Social Services Program Specialist II in Provider Support	DHCFP	100%	Oversight of FA provider support staff.	LG 35 $32.42 $87,534.00
Hearings Officer State of Nevada Dept. of Administration	Dept. of Administration Hearings Unit	2 @100%	Hear the appeals, decide, and write decisions. If taken to court, becomes DAG and DHCFP function.	LG 36 $33.91 $183,114.00

5 Description of Nature and Scope of Activities and Methods

DHCFP has completed a SMHP that details the nature and scope of the activities and methods for the Nevada plan for payment of incentives to Providers that adopt, implement, or upgrade to certified EHR systems and become meaningful users of the technology. The SMHP also details the current HIT landscape and articulates a future HIT landscape for its "To-Be" environment. The SMHP includes a roadmap for activities that will enable the actions from the current environment to the future environment.

5.1 Scope of Activities and Methods

As a result of the approval of this IAPD, the implementation of NPIP will be undertaken. The activities involved in this project are as follows:

Administration:

- Complete the design, development, and implementation of the NPIP registration and attestation system;
- Complete the internal DHCFP organizational and staffing planning;
- Monitor contractor performance (if external contractor required);
- Conduct reporting of actual and estimated expenditures;
- Implement quality assurance activities;
- Update the SMHP and IAPD as required;
- Develop RFPs for outsourced services (if required):
    - Detailed data analysis, evaluation and oversight, and auditing and reporting capabilities;
    - Evaluation of EHR incentive program (IV&V) and impact to DHCFP cost/quality outcomes; and
    - Business process modeling/engineering.

Oversight:

- Implement auditing and appeals; and
- Track and monitor provider incentive payments.

EHR Promotion:

- Execute provider outreach and education training;
- Update DHCFP websites with EHR incentive program information;
- Engage DHCFP public relations office participation; and
- Collaborate with Statewide HIE and stakeholders.

6 HIT Roadmap and Activity Schedule

The following table shows the major activities and milestones to move DHCFP from "As-Is" to "To-Be" status. The following table illustrates the HIT Roadmap and Activities, including milestones for DHCFP. Some activities occur every quarter and are shown in the activity list, but only appear as milestones in their first occurrence.

Table 4: HIT Roadmap and Activities

Date	Activity (◆ = Milestone)
2011 – 2nd Quarter April/May/June	• Define roles for Medicaid Business Units in the NPIP. • Finalize program requirements for the NPIP. • Complete and submit the SMHP and IAPD documents to CMS. • Continue coordinated outreach efforts with the REC and Statewide HIE.
2011 – 3rd Quarter July/August/September	• Begin development of MMIS system replacement Request for Proposal (RFP). ◆ Begin State procurement process for software application to be used for the NPIP eligibility system. • Complete training sessions for DHCFP. • Continue coordinated outreach efforts with the REC and Statewide HIE.
2011 – 4th Quarter October/November/December	• Review CMS requirements for Meaningful Use. • Continue coordinated outreach efforts with the REC and Statewide HIE. ◆ Reach an agreement on roles and responsibilities with Statewide HIE.
2012 – 1st Quarter January/February/March	• Hire and train additional staff to be used for the NPIP. • Notify all Medicaid Providers of NPIP program changes and effective dates. • Review and revise State policy manual. ◆ Implement vendor software for the NPIP eligibility system. ◆ Complete testing of software application to be used in the NPIP. ◆ Implement NPIP software application and create links from other Medicaid websites. ◆ Conduct training sessions for Providers. • Data warehouse – plan for integration with MMIS and Statewide HIE. • Finalize an agreement on roles and responsibilities with Statewide HIE. • Continue coordinated outreach efforts with the REC and Statewide HIE.
2012 – 2nd Quarter April/May/June	• Publish NPIP manual and user guide. • Review and revise the Verification and Audit Strategy. ◆ Start accepting/approving NPIP applications for Providers (Year 1/Group 1). ◆ Implement pre-payment verifications and audits. • Conduct pre-payment verifications and post-payment audits. • Continue coordinated outreach efforts with REC in addition to Statewide HIE. • Develop requirements of the RFP for the interface to the Statewide HIE.
2012 – 3rd Quarter July/August/September	◆ Make NPIP payments (Year 1/Group 1). • Approve NPIP applications for payment (Year 1/Group 2). • Conduct pre-payment verifications and post-payment audits. • Review and revise audit selection criteria and Verification and Audit Strategy. • Continue coordinated outreach efforts with REC in addition to Statewide HIE. • Release RFP for development of the interface to the Statewide HIE.

Date	Activity (◆ = Milestone)
2012 – 4th Quarter October/November/December	• Make NPIP payments (Year 1/Group 2). • Approve NPIP applications for payment (Year 1/Group 3). • Conduct pre-payment verifications and post-payment audits. • Review CMS requirements for 2013 program changes. • Develop requirements for any changes to the NPIP software application. • Review and modify the NPIP manual and user guide as needed. • Notify all Medicaid Providers of changes and effective dates. ◆ Develop Verification and Audit Strategy for year 2013 Meaningful Use and other program requirements. • Continue coordinated outreach efforts with REC in addition to Statewide HIE. • Complete development and testing of the interface to the Statewide HIE. • Implement interfaces with the Statewide HIE.
2013 – 1st Quarter January/February/March	• Make NPIP payments (Year 1/Group 3). • Approve NPIP applications for payment (Year 1/Group 4). • Conduct pre-payment verifications and post-payment audits. • Review and revise State policy manual. • Finalize Verification and Audit Strategy for year 2013 Meaningful Use and other program requirements. • Update training materials on Year 2 requirements and post to the Medicaid websites. • Conduct training sessions for Providers. • Continue coordinated outreach efforts with REC in addition to Statewide HIE.
2013 – 2nd Quarter April/May/June	• Make NPIP payments (Year 1/Group 4). ◆ Approve NPIP applications for payment (Year 2/Group 1). First Meaningful Use group. • Conduct pre-payment verifications and post-payment audits. • Continue coordinated outreach efforts with REC in addition to Statewide HIE.
2013 – 3rd Quarter July/August/September	◆ Make NPIP payments (Year 2/Group 1). First Meaningful Use group. • Approve NPIP applications for payment (Year 2/Group 2). • Conduct pre-payment verifications and post-payment audits. • Continue coordinated outreach efforts with REC in addition to Statewide HIE.
2013 – 4th Quarter October/November/December	• Make NPIP payments (Year 2/Group 2). • Approve applications for payment (Year 2/Group 3). • Conduct pre-payment verifications and post-payment audits. • Review and revise audit selection criteria and Verification and Audit Strategy. • Continue coordinated outreach efforts with REC in addition to Statewide HIE. ◆ Award RFP contract for MMIS system replacement/negotiate contract.

7 Proposed Budget

DHCFP presents the following budget spreadsheet for this IAPD. This budget includes the proposed costs for the total payment of the incentives to Providers. This budget also includes costs for administration, oversight, and adoption activities that will accelerate success of NPIP and facilitate the adoption and MU of certified EHR technology. This budget does not duplicate MU technical assistance efforts conducted by the Office of the National Coordinator (ONC) funded regional extension centers, workforce grantees, Beacon Grantees or other federally-funded projects whose target population is the same. This budget also does not include any costs associated with the development of the Statewide HIE.

The attached budget spreadsheet represents the categories of costs for this program throughout 2014. As this program develops and implementation continues, DHCFP will submit updated information to assure CMS has the most accurate cost information.

7.1 Cost to Implement and Administer Incentive Payments

The information in the budget spreadsheet represents costs in nine (9) different categories:

1. **Procurement or Acquisition** – These are costs associated with the procurement process. As the State normally provides these services, this IAPD has no costs associated with this category.
2. **State Personnel** – These are costs for additional state personnel resources necessary to administer the incentive program. The need for additional personnel is anticipated for the administration and oversight of the program. The Personnel Resource Statement values from Table 3 are included in the budget spreadsheet.
3. **Contractor Services** – These are costs for contracted services for the Web-based hosted SaaS solution. These costs include the following:
    - SLR Implementation Services;
    - Ongoing Maintenance and Support;
    - Business Process Re-engineering;
    - IV&V; and
    - Developing Data Sharing and Business Associate Agreements (Legal support).
4. **Hardware, Software, and Licensing** – These are costs for the purchase of hardware and software. As the State is procuring a SaaS solution through contractor services, this IAPD has no costs associated with this category.
5. **Equipment and Supplies** – These are costs for operating supplies and equipment needed to administer the program.
6. **Training and Outreach** – These are costs associated with staff development and Provider education.
7. **Travel** – These are costs associated with staff travel costs for administration and oversight of the program.

8. **Administrative Operations** – These are costs associated with costs to the State for operating expenses, indirect costs, and cost allocations for the program.
9. **Miscellaneous Expenses** – These are costs associated with membership dues the State incurs as part of a multi-state collaborative on HIT.

The following budget spreadsheet represents the categories and costs to implement and administer the incentive program.

Table 5: Cost to Implement and Administer Incentive Payments

Cost Category	Total	FFY 10-11 (partial)	FFY 11-12	FFY 12-13	FFY 13-14	FFY 14-15 (partial)
Procurement or acquisition	$ -	$ -	$ -	$ -	$ -	$ -
State personnel	$ 3,346,646	$ 209,163	$ 878,488	$ 1,003,998	$ 1,003,998	$ 250,999
Contractor services	$ 6,118,165	$ 61,938	$ 2,048,785	$ 1,772,752	$ 1,772,752	$ 461,938
Hardware, software, maintenance, and licensing	$ -	$ -	$ -	$ -	$ -	$ -
Equipment and supplies	$ 30,041	$ 6,813	$ 7,147	$ 7,147	$ 7,147	$ 1,787
Training and outreach	$ 27,618	$ 8,085	$ 6,010	$ 6,010	$ 6,010	$ 1,503
Travel	$ 56,825	$ 14,084	$ 13,151	$ 13,151	$ 13,151	$ 3,288
Administrative operations	$ 229,443	$ 18,975	$ 65,417	$ 64,467	$ 64,467	$ 16,117
Miscellaneous expenses	$ 34,000	$ 8,000	$ 8,000	$ 8,000	$ 8,000	$ 2,000
TOTAL	$ 9,842,737	$ 327,058	$ 3,026,998	$ 2,875,525	$ 2,875,525	$ 737,631

7.1.1 Estimate of Prospective Cost Distribution to the State and Federal Funding Sources and the Proposed Procedures for Distributing Costs

The planning and implementation funding cost distribution is a 90% federal funding with 10% DHCFP funding. These funds will be distributed using the standard operating Medicaid financial management procedures for DHCFP.

Table 6: Cost Distribution to the State and Federal Funding Sources

Cost Category	Total	FFY 10-11 90%	FFY 10-11 10%	FFY 11-12 90%	FFY 11-12 10%	FFY 12-13 90%	FFY 12-13 10%	FFY 13-14 90%	FFY 13-14 10%	FFY 14-15 90%	FFY 14-15 10%
Procurement or acquisition	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
State personnel	$ 3,346,646	$ 188,247	$ 20,916	$ 790,639	$ 87,849	$ 903,598	$ 100,400	$ 903,598	$ 100,400	$ 225,899	$ 25,100
Contractor services	$ 6,118,165	$ 55,744	$ 6,194	$ 1,843,907	$ 204,879	$ 1,595,477	$ 177,275	$ 1,595,477	$ 177,275	$ 415,744	$ 46,194
Hardware, software, maintenance, and licensing	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Equipment and supplies	$ 30,041	$ 6,132	$ 681	$ 6,432	$ 715	$ 6,432	$ 715	$ 6,432	$ 715	$ 1,608	$ 179
Training and outreach	$ 27,618	$ 7,277	$ 809	$ 5,409	$ 601	$ 5,409	$ 601	$ 5,409	$ 601	$ 1,352	$ 150
Travel	$ 56,825	$ 12,676	$ 1,408	$ 11,836	$ 1,315	$ 11,836	$ 1,315	$ 11,836	$ 1,315	$ 2,959	$ 329
Administrative operations	$ 229,443	$ 17,078	$ 1,898	$ 58,875	$ 6,542	$ 58,020	$ 6,447	$ 58,020	$ 6,447	$ 14,505	$ 1,612
Miscellaneous expenses	$ 34,000	$ 7,200	$ 800	$ 7,200	$ 800	$ 7,200	$ 800	$ 7,200	$ 800	$ 1,800	$ 200
TOTAL	$ 9,842,737	$ 294,352	$ 32,706	$ 2,724,298	$ 302,700	$ 2,587,972	$ 287,552	$ 2,587,972	$ 287,552	$ 663,868	$ 73,763

7.2 Planned Annual Payment Amounts

7.2.1 Eligible Professionals

The estimated payments to professionals eligible for the program were computed using assumptions taken directly from the Final Rule, CMS-0033-F, pages: 741-743. As seen in the table below based on the Final Rule assumptions, DHCFP expects to issue payments that total $13,567,957 between 2012 and 2014 to EPs under the program.

Table 7: EP Payments to be Issued Between 2012 and 2014

Nevada Number of Physicians, PA's, NP's, Dentists	Nevada Number of Pediatricians	Number of Physicians Who Meet the Volume Requirements	Number of Pediatricians Who Meet the Volume Requirements
6,201	307	1,240	154

Federal Estimate of Percentage Who Will Receive Payments in First Year (Low Scenario)	Number of Nevada EP's to Receive Payments at $21,250 Level	Number of Nevada Pediatricians to Receive Payments at $21,250 Level	Number of Nevada Pediatricians to Receive Payments at $14,167 Level	Estimated Nevada Payments in 2012
15.10%	188	12	12	$4,420,004

Federal Estimate of Percentage Who Will Receive Payments in Second Year (Low Scenario)	Number of Nevada EP's to Receive payments at $21,250 Level	Number of Nevada Pediatricians to Receive Payments at $21,250 Level	Number of Nevada Pediatricians to Receive Payments at $14,167 Level	Number of Nevada EP's to Receive Payments at $8,500 Level	Number of Nevada Pediatricians to Receive Payments at the $8,500 Level	Number of Nevada Pediatricians to Receive Payments at $5,667 Level	Estimated Nevada Payments in 2013
24.00%	111	7	7	187	11	11	$4,354,965

Federal Estimate of Percentage Who Will Receive Payments in Third Year (Low Scenario)	Number of Nevada EP's to Receive payments at $21,250 Level	Number of Nevada Pediatricians to Receive Payments at $21,250 Level	Number of Nevada Pediatricians to Receive Payments at $14,167 Level	Number of Nevada EP's to Receive Payments at $8,500 Level	Number of Nevada Pediatricians to Receive Payments at the $8,500 Level	Number of Nevada Pediatricians to Receive Payments at $5,667 Level	Estimated Nevada Payments in 2014
30.80%	85	6	6	297	18	18	$4,792,988

7.2.2 Eligible Hospitals

The estimated payments to hospitals eligible for the program were computed using the calculations provided in the CMS regulations at 42 CFR.310(f). DHCFP used the CMS calculation provided in the regulations and generated estimated payments for each EH. DHCFP also plans to issue incentive payments to EHs by paying 50% in year 1, 40% in year 2 and 10% in year 3. As seen in the table below DHCFP expects to issue payments that total $38,223,039 to EHs during the program. Even though each EH will have a different payment amount and will enter the program at different times, the total estimated EH payment amount was distributed based on the 50% / 40% / 10% payout schedule to determine cost per year.

Table 8: EH Payments to be Issued Between 2012 and 2014

Distribution	Year 1: 50%	Year 2: 40%	Year 3: 10%	Total
Hospital Payments	**$ 19,111,519**	**$ 15,289,216**	**$ 3,822,304**	**$38,223,039**

7.2.3 Total

As seen in the table below based on the Final Rule assumptions, DHCFP expects to issue payments that total $51,790,996 between 2012 and 2014 to EPs/EHs under the program.

Table 9: Total EP/EH Payments to be Issued Between 2012 and 2014

Year	2012	2013	2014	Total
EP Payments	$ 4,420,004	$ 4,354,965	$ 4,792,988	$ 13,567,957
EH Payments	$ 19,111,519	$ 15,289,216	$ 3,822,304	$ 38,223,039
TOTAL	**$ 23,531,523**	**$ 19,644,181**	**$ 8,615,292**	**$ 51,790,996**

8 Security and Interface Requirements for All State HIT Systems and Related Systems

8.1 Specific Security for Nevada

The specific security requirements for the NPIP are expected to be identical to those in the MMIS Takeover RFP, as executed currently. The following excerpt from the MMIS Security Plan show the specific standards being proposed and followed.

> This sections lists the controls required by the system and will be cross-referenced to HIPAA, ARRA, HITECH, State of Nevada standards and applicable Federal and State laws.
>
> As noted in this Security Plan, NV MMIS controls are selected from a catalog of all security controls as required by NIST SP 800-53 (Rev. 3, dated June 2009). The controls were selected as directed by DHCFP, additional controls were selected as part of the risk assessment in section 4.3.
>
> There is an assurance requirement that the security control is in effect and meets explicitly identified functional requirements in the control statement. NIST provides a description of the functional properties of the control with sufficient detail to permit analysis and testing of the control. HPES as the control developer/implementer includes as an integral part of the control, assigned responsibilities and specific actions supporting confidence that when the control is implemented, it will meet its required function or purpose. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.
>
> For security controls required by contract, the focus is on actions supporting confidence in the correct implementation and operation of the control. While flaws are still likely to be uncovered, HPES, the control implementer will incorporate, as part of the control, specific capabilities and produces specific documentation supporting increased confidence that the control meets its required function or purpose. A summary of the RFP required controls implemented are as in the table below. Additional controls were selected based on the risk assessment in section 4.3.

Control	Name (Based on NIST 800-53, R.3, Aug-2009)	Base line	Values	NIST SP 800-66 HIPAA Xref Note 1	RFP Req	NV DOIT Standards	Comments
AC Family: Access Control (Class: Technical)							
AC-1	Access Control Policy and Procedures (For a description of the controls refer to NIST 800-53, for brevity, they were not included in this table.)	LMH		164.308(a)(3)(i) 164.308(a)(3)(ii)(A) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.312(a)(1)		4.60B.6.0.1K 4.63A.6.0	

AC-2	Account Management	LMH	Sponsors review sys/user master list quarterly. 11.4.3.4 - Process user ID changes and additions within three (3) working days of each request. 11.4.3.5 - Process user ID deletions within one (1) working day of each request.	164.308(a)(3)(ii)(A) 164.308(a)(3)(ii)(B) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.308(a)(5)(ii)(C) 164.312(a)(2)(i) 164.312(a)(2)(ii)	11.4.1.3 11.4.1.4 11.4.3.4 11.4.3.5 12.2.2.4	4.60B.6.0.1G 4.60B.6.0.1I 4.60B.6.0.1J 4.62C.6.0.4 4.63A.6.0.1A	
AC-3	Access Enforcement	LMH	PSO evaluates access priv's annually on a sample basis	164.308(a)(3)(ii)(A) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.310(a)(2)(iii) 164.310(b) 164.312(a)(1) 164.312(a)(2)(i) 164.312(a)(2)(ii) 164.312(a)(2)(iv)		4.31A.6.0.1 4.31A.6.0.2 4.60B.6.0.1A 4.60B.6.0.1B 4.60B.6.0.1F 4.60B.6.0.1H 4.62C.6.0.2 4.62C.6.0.6 4.63A.6.0.1B	

AC-3(3)	Access Enforcement - Non-Discretionary Access Control (NDAC)	Opt.	Role-based		11.4.1.5		
AC-3(6)	Access Enforcement – Encrypts or Stores in Secure Location	Opt.	Data on Tapes				
AC-4	Information Flow Enforcement	MH	Firewall must employ packet filtering. High traffic firewalls must use stateful inspection. Firewall must be able to use NAT.	164.308(a)(3)(ii)(A) 164.308(a)(4)(ii)(B) 164.310(b)	11.3.1.10 11.4.1.6 11.4.1.14 14.2.3.8	4.62C.6.0.6. CliC 4.63A.6.0.1C 4.63A.6.0.1F 4.63A.6.0.1G 4.64A.6.0B	
AC-5	Separation of Duties	MH		164.308(a)(3)(i) 164.308(a)(4)(i) 164.308(a)(4)(ii)(A) 164.312(a)(1)	3.5.10.2	4.04D.6.0F 4.60B.6.0.1H	
AC-6	Least Privilege	MH		164.308(a)(3)(i) 164.308(a)(4)(i) 164.308(a)(4)(ii)(A) 164.312(a)(1)	11.3.1.2 11.4.1.5	4.60B.6.0.1H	

AC-11	Session Lock	MH	20 Minutes of Inactivity	164.310(b) 164.312(a)(2)(iii)			
AC-16	Security Attributes	Opt.		164.310(b)			
AC-17	Remote Access	LMH		164.310(b)		4.62C.6.0.1 4.62C.6.0.5	
AC-18	Wireless Access	MH	Default settings not allowed. Auth to WLAN not access to wired net. All wireless traffic must be encrypted.			4.62C.6.0.8A 4.62C.6.0.8B 4.62C.6.0.8D	
AC-19	Access Control for Mobile Devices	LMH		164.310(b)			
AC-22	Publicly Accessible Content	LMH				4.60B.6.0.1D	Added by the Risk Assessment in section 4.3
AT – Awareness and Training							
AT-1	Security Awareness and Training Policy and Procedures	LMH		164.308(a)(5)(i)		4.65A.6.0ff	

AT-2	Security Awareness	LMH		164.308(a)(5)(i) 164.308(a)(5)(ii)(A) 164.308(a)(5)(ii)(B)		4.05A.6.0	
AT-3	Security Training	LMH		164.308(a)(5)(i)	11.3.1.9 11.3.1.16 12.3.1.11	4.05A.6.0C	
AT-4	Security Training Records	LMH	Emp. Must ack. training	164.308(a)(5)(i)		4.05A.6.0D	
AT-5	Contacts with Security Groups and Associations	Opt.		164.308(a)(5)(i) 164.308(a)(5)(ii)(A)			
AU Family: Audit and Accountability (Class: Technical)							
AU-1	Audit and Accountability Policy and Procedures	LMH		164.312(b)		4.60B.6.0.2A 4.60B.6.0.2D 4.60B.6.0.2E 4.60B.6.0.2F 4.60B.6.0.2G	

AU-2	Auditable Events	LMH	Firewall must log traffic. Retain suspicious events 1 year. 11.4.1.15 Maintain audit trails for all data received or transmitted.	164.308(a)(5)(ii)(C) 164.312(b)	11.4.1.8a 11.4.1.8b 11.4.1.9 11.4.1.15	4.60B.6.0.2 4.63A.6.0.1D 4.64A.6.0G	
AU-3	Content of Audit Records	LMH		164.312(b)			
AU-4	Audit Storage Capacity	LMH		164.312(b)			
AU-6	Audit Review, Analysis, and Reporting	LMH		164.308(a)(1)(ii)(D) 164.308(a)(3)(ii)(A) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(5)(ii)(C) 164.312(b)	14.2.3.7		
AU-6(2)	Audit Review, Analysis, and Reporting - Automated Alerts	Opt.			14.2.3.7		
AU-7	Audit Reduction and Report Generation	MH		164.308(a)(1)(ii)(D) 164.312(b)		4.10A.6.0E	
CA Family: Certification, Accreditation, and Security Assessments (Class: Management)							
CA-1	Security Assessment and Authorization Policies and Procedures	LMH		164.308(a)(8)			
CA-2	Security Assessments	LMH		164.308(a)(2) 164.308(a)(8)		4.09A.6.0A 4.09A.6.0B 4.09A.6.0E	
CA-3	Information System Connections	LMH		164.308(b)(1) 164.308(b)(4) 164.314(a)(2)(ii)			
CA-6	Security Authorization	LMH		164.308(a)(2) 164.308(a)(8)			
CA-7	Continuous Monitoring	LMH		164.308(a)(1)(ii)(D) 164.308(a)(8)			
CM Family: Configuration Management (Class: Operational)							
CM-1	Configuration Management Policy and Procedures	LMH				4.63A.6.0.3	
CM-4	Security Impact Analysis	LMH			3.5.10.3	4.09A.6.0C 4.30A.6.0A	

CM-5	Access Restrictions for Change	MH			3.5.8 3.5.10.2 11.3.1.1 11.3.2.2 11.3.3.2 11.4.1.8a 11.4.1.8c	4.30A.6.0H 4.60B.6.0.2C	
CM-6	Configuration Settings	LMH	Non-dedicated OS must be hardened. Firewall Sys Admin must be trained to harden OS.			4.63A.6.0.1E1 4.63A.6.0.1H1	Added by Section 4.3
CM-8	Information System Component Inventory	LMH		164.310(d)(1) 164.310(d)(2)(iii)		4.10A.6.0C	Added by Section 4.3
CP Family: Contingency Planning (Class: Operational)							
CP-1	Contingency Planning Policy and Procedures	LMH		164.308(a)(7)(i)			
CP-2	Contingency Plan	LMH		164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.308(a)(7)(ii)(D) 164.308(a)(7)(ii)(E) 164.310(a)(2)(i) 164.312(a)(2)(ii)	11.5.1 11.5.2.1 11.5.4.1 11.5.4.2 11.5.4.3 11.5.4.4	4.07A.6.0A 4.07A.6.0B 4.07A.6.0D 4.32A.6.0A1C4 4.32A.6.0A2C 4.32A.6.0A2D	
CP-3	Contingency Training	LMH		164.308(a)(7)(ii)(D)		4.07A.6.0E 4.32A.6.0A2F	
CP-4	Contingency Plan Testing and Exercises	LMH	Restore testing semi-annual or sooner.	164.308(a)(7)(ii)(D)	11.5.4.6	4.07A.6.0F 4.32A.6.0A2C	
CP-6	Alternate Storage Site	MH		164.308(a)(7)(ii)(B) 164.310(a)(2)(i)		4.07A.6.0C	
CP-7	Alternate Processing Site	MH		164.308(a)(7)(ii)(B) 164.310(a)(2)(i)			
CP-8	Telecommunications Services	MH		164.308(a)(7)(ii)(B)			
CP-9	Information System Backup	LMH	Agency Defined frequency. Must maintain multi-generations of backups, at least one stored off-site.	164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B) 164.310(d)(2)(iv) 164.312(c)(1)		4.32A.6.0A 4.32A.6.0A1B	Added by Risk Assessment see sec. 4.3
CP-9(1)	Information System Backup - Testing	MH				4.32A.6.0A1C3	
CP-10	Information System Recovery and Reconstitution	LMH		164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C)		4.32A.6.0A2A	

NOTE: This table continues on for several more pages. The full Security Plan is available on request.

8.2 Federal Requirements for Security

The Secretary of Health and Human Services adopted the following standards for health information technology to protect electronic health information created, maintained, and exchanged:[1]

(a) Encryption and decryption of electronic health information—

(1) General. Any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140–2 as shown in the table below:

Approved Security Functions	Algorithms
Symmetric Key	Advanced Encryption Standard (AES), Triple-DES Encryption Algorithm (TDEA) and Escrowed Encryption Standard (EES)
Asymmetric Key	Digital Signature Standard (DSS) – DSA, RSA and ECDSA
Secure Hash Standard	SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512
Random Number Generation	Deterministic Random Number Generators listed in NIST FIPS 140-2 Annex C
Message Authentication	Triple-DES MAC, CMAC, CCM, GCM, GMAC and HMAC
Key Management	NIST Recommendation for Key Derivation Using Pseudorandom Functions, SP 800-108

(2) Exchange. Any encrypted and integrity protected link.

(b) Record actions related to electronic health information.

The date, time, patient identification, and user identification must be recorded when electronic health information is created, modified, accessed, or deleted; and an indication of which action(s) occurred and by whom must also be recorded.

(c) Verification that electronic health information has not been altered in transit.

A hashing algorithm with security strength equal to or greater than SHA–1 (Secure Hash Algorithm (SHA–1) as specified by NIST in FIPS PUB 180–3 (October, 2008)) must be used to verify that electronic health information has not been altered.

(d) Record treatment, payment, and health care operations disclosures.

The date, time, patient identification, user identification, and a description of the disclosure must be recorded for disclosures for treatment, payment, and health care operations, as these terms are defined at 45 Code of Federal Regulations (CFR) 164.501.

[1] 45 CRF Part 170 – Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology; Final Rule

8.3 Public Key Infrastructure

Data exchange over the Internet requires a certain level of security capabilities to protect against any threats to the communication or integrity of information. In the health care vertical, since patient privacy is one of the most critical issues, personal health information (PHI) needs to be protected effectively with the highest level of security capabilities. Many technologies have been developed and adopted to address security issues when using the Internet, including Public Key Infrastructure (PKI) to ensure a standard-based, secure, encrypted exchange of sensitive clinical information across health care networks.

8.4 Public Key Infrastructure and X.509 Certificate

PKI is a set of network services that support: 1) creation of a public and private cryptographic key pair via a trusted authority; 2) management (distribution and revocation) of an asymmetric cryptography key pair; 3) security of transmitted data; and 4) validation of end-users and end-systems.

X.509 is the standard deployment of PKI (X.509 digital certificates). These PKI mechanisms can be used to: 1) create secure networks over the unsecure public Internet; 2) ensure the integrity and confidentiality of PHI exchanged across networks; and 3) ensure authorized access to PHI by validating a user's identity.

Table 10: PKI Functionality

Functionality	Description
Authentication	Validating the identity of end systems and users (i.e., "verifying they are who they say they are") through the digital signature mechanism.
Integrity	Assuring the message integrity (i.e., "the transferred message has not been compromised in any way from the original message") through the digital signature mechanism.
Confidentiality	Ensuring the confidentiality of the message (i.e., "only the intended recipient can read the message") through message encryption.
Non-repudiation	Ensuring the uniqueness and originality of trading partners (i.e., "the transferred message has been sent and received by the parties claiming to have sent and received the message") through the digital signature mechanism.

8.5 Authentication, Authorization, Access Control and Auditing (4A) Using PKI

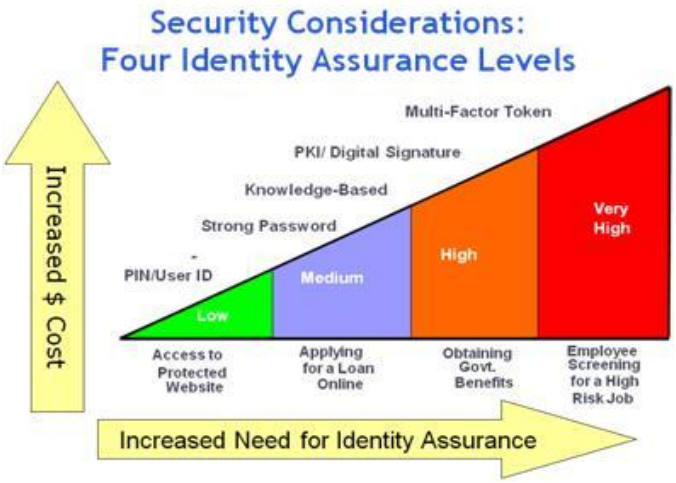
In order to provide secure health care information exchange across organizations, several operational difficulties need to be addressed when implementing the electronic access to patient clinical information:

1. Authorization - Establishing and managing a list of authorized persons: strong identity proofing procedures during the process of credential issuance to users. Every user needs to present identifying materials and information such as a government issued photo ID and notarization.

2. Authentication - Verifying the identity of the authorized users accessing clinical information: identity Assurance Level 3 or Level 4 for authentication. Level 3 authentication is based on the proof of possession of a X.509 digital certificate. Level 4 authentication is similar to Level 3 except it requires hardware tokens such as smart cards, USB tokens, or key fobs.
3. Access Control - Appropriately limiting authorized users' access to PHI based on their roles and privileges: role-based access control (RBAC) to provide health care organizations with a fine-grained access control to PHI under local control. (This is discussed in detail in the following section.)
4. Auditing - Logging audit trails on every access to PHI and reviewing/examining audit trails to assess the adequacy of systems control on established security policies: vendors should implement a standard-based, IHE ATNA profile compliant audit record repository to support auditing. Every transaction between trading partners and health information systems is logged in one or more audit repositories and is available to security officers for review/assessment.

8.6 User Authorization and Authentication

For stronger user identity assurance, user identity credentials supporting Assurance Levels 3 and 4 are recommended (shown in the diagram below): HSPD-12 and FIPS201 compliant: Vendors should be compliant with the requirements of Homeland Security Presidential Directive 12 (HSPD-12) for standardized identification credentials. Vendor credentials (software certificates, hardware tokens, or smart cards) comply with Federal Information Processing Standard #201 (FIPS201) including smart card technology, biometrics, and certificate validation.



Furthermore, it is recommended to leverage Federated Identity Management technology to ensure provider (user) authentications. In this model, there is no centralized shared provider directory. A SAML-based federated identity for a Provider will be generated locally and exchanged/used globally between stakeholders and further role/privilege based access control decision will be made locally based on their own local security and privacy policies.

8.7 Secure Data Transmission

For secure transactions, Web Services technology together with PKI technology is strongly recommended. A secure channel is established over TLS and messages (containing PHI) that are encrypted and digitally signed when they are transmitted from one system to another health information system. Communication between systems and end secure nodes is a Web Services call built on top of a SOAP and SAML stack.

PKI cryptography technology is recommended for two-level security (for secure routing): transport-level security and message-level security. SSL/TLS protocol is used to provide encryption of the communication channel and secure authentication (mutual authentication) of the server. For message-level security, WS-Security should be utilized to encrypt the content of the message (SOAP message). This is aligned with the approaches adopted by ONC/NHIN architecture.

8.8 Other Security Considerations

The following security recommendations and considerations are under review by DHCFP to be utilized to protect critical health information:

1. Integrity and access controls to and for Medicaid data: No unauthorized modification operation should be allowed on databases containing PHI. Databases containing PHI should be encrypted, including encrypted data (at rest);
2. Confidentiality: Any query result is accessed only by authorized persons or organizations. All transactions involving PHI should be logged; and
3. Preventing unauthorized disclosure of the data: During transmission, all communication between DHCFP systems and external systems should be encrypted and logged.

To ensure the security recommendations and considerations described above, two security controls are recommended: physical access control and technical security control.

Physical Access Control: Physical access to computers and software systems should be restricted and audited:

- Computer screens (monitors) should have a pre-defined time-out feature – for example, screen-locked after no activity for 60 seconds; and
- Passwords (database and computers) should be properly and securely managed to prevent unauthorized access or manipulation of the system.

Technical Security Control:

- Firewall settings for access control;
- SQL Query restriction: No direct database access is allowed from outside the network;
- Node authentication verification: Client/server verification (authentication) is performed based on X.509 based PKI infrastructure over a secured Virtual Private Network tunnel:
    - Only the systems that have certificates legitimately signed by trusted partners will be able to access the servers;
    - Certificates are generated based on RSA public-key authentication algorithm. A 1024 (or 2048 bits for stronger encryption) bit RSA private key for each certificate is generated for message encryption for secure communication; and
    - X.509 key/certificate pair should be kept securely in a local directory.

8.9 Disaster Recovery Plan

The specific disaster recovery plan and requirements for the NPIP are expected to be identical to those in the MMIS Takeover RFP, as executed currently. As noted in the Security and Interface Requirements for All State HIT Systems and Related Systems section above, the disaster recovery plan and requirements follow the MMIS requirements. The full Security Plan is available upon request.

9 Unspent Planning Advance Planning Document (P-APD) Funds

The P-APD was approved on February 23, 2010 for total computable costs not to exceed $1,171,247 at the 90% federal financial participation (FFP) rate, for a federal total computable share of $1,054,122. Including actuals through quarter-ending March 31, 2011 along with projections through June 30, 2011, total expenditures amount to $859,154.86 for a 90% federal share of $773,239.37. Therefore as of June 30, 2011, the unspent P-APD total is anticipated to be $312,092.14 and the unspent P-APD federal share is anticipated to be $280,882.93. The table below shows a summary of the total P-APD expenditures. DHCFP anticipates P-APD funding will be closed as of June 30, 2011, pending approval of IAPD funding.

Table 11: Unspent P-APD Funds

P-APD Budget Reconciliation				
P-APD Approved Category	**Amount Requested**	**Amount Expended [1]**	**Difference**	**Carry-Forward to IAPD**
Planning Resources/Personnel	$451,764.00	$179,485.19	$272,278.81	$0.00
Planning Contractor Resources	$675,000.00	$653,460.50	$21,539.50	$0.00
Planning Other Expenses [2]	$44,483.00	$26,209.17	$18,273.83	$0.00
TOTALS	**$1,171,247.00**	**$859,154.86**	**$312,092.14**	**$0.00**

[1] Amount Expended includes projections through quarter-ending June 30, 2011, when use of planning funds is expected to end, pending approval of the IAPD.

[2] Other Expenses include program-specific dues, travel, equipment, and miscellaneous operating expenses in support of the program.