Vermont Health Connect: Exchange Options for 2017

An Assessment of the Alternatives

November 2, 2015

Appendices:

- **A.** Vendor Questionnaire
- **B.** Questions for States
- **C.** State Exchange Interview Notes
- **D.** VHC Cost Estimate Summaries
- **E.** CMS IT Decommissioning Data Retention Planning

  SBM IT Decommissioning Data Retention Planning
- **F.** Federal Exchange Fee Range

  Net Premium and Estimated Federal Fee by Family Size and Income

Appendix A:

Vendor Questionnaire

State of Vermont Vendor Questionnaire

Description		Mark Only 1 column with "X" per requirement			
Criteria	**Capability**	**Provided in Out-Of-Box Solution**	**Partially Provided Solution (Provide details)**	**Customizable Solution**	**No Solution**
Legal	Comply with all CMS SHOP related components of regulation 45 CFR				
Legal	Ability to comply with VT requirements including but not limited to: 33 V.S.A 1802, HBEE Rule 34.00, 36.00, 40.00, 41.00, 43.00 http://legislature.vermont.gov/statutes/ http://dcf.vermont.gov/sites/dcf/files/pdf/esd/rules/Non-Annotated.pdf				
Security	Comply with security provisions consistent with CMS regulation 45 CFR 155.260. 270. 280.				
Security	Provide audit logging and reporting capability.				
Capability	Provide ability to create, and manage unique identifiers for each employer, employee, and broker participating in the exchange.				
Capability	Provide ability to prohibit and manage creation of duplicate accounts.				
Capability	Provide the capability for employers to browse available options without creating a system account.				
Capability	Provide an employer and employee application process that collects all necessary data to execute SHOP transactions through web portal, call center, or via paper application.				
Capability	Provide the capability for an employer and employee to edit, save and return to the application at any point.				
Capability	Provide multiple methods for an employer to build and manage an employee roster (e.g. manual entry, file upload, etc.).				
Capability	Provide ability to differentiate/track full-time versus part-time/hourly employees in the employee roster.				
Capability	Allow authorized brokers to complete and manage employer applications on behalf of the employer.				
Capability	Provide ability to associate or disassociate employee and employer records.				
Capability	Provide calculator that estimates				

	employer's plan cost based on applicable rating factors (employees', age, geography, family size etc.) and employee choice model selected.				
Capability	Provide ability for employer to select plans/tiers, contribution amounts, and to display plan costs and availability.				
Capability	Provide ability to display a cost comparison of available plans.				
Capability	Provide ability to conduct an eligibility determination as to whether an employer meets size, location and employee coverage requirements to utilize the SHOP Exchange.				
Capability	Provide the capability to initiate a manual or automated verification process for employer, or employee data (EIN, SSN, etc…).				
Capability	Provide the ability to upload supporting employer eligibility documentation.				
Capability	Provide ability for employer and employee enrollment or termination, both voluntary and involuntary, and ability to seamlessly process with carriers and premium processors.				
Capability	Provide ability to process and manage small business tax credit form.				
Capability	Provide the capability to process and manage an appeal request, and support the transmission of complaint / appeal data to authorized third-parties.				
Capability	Provide options for confidentiality (e.g. such as appeal requests to hide consumer name, or VIP's) and allow access to cases by specified authorized users.				
Capability	Provide capability to flag accounts for alerting Call Center for special cases.				
Capability	Provide call center capability to enter cases notes and to track and manage requests.				
Capability	Provide notification of enrollment, termination, or verification requests, to both employer and employee.				
Capability	Provide ability to generate notices to CMS regarding an employee's disenrollment / change from a qualified health plan through the Exchange.				
Capability	Provide ability to process premium invoices both itemized and aggregated.				
Capability	Provide the ability to process invoice payments via eCheck, EFT, paper check, credit cards, and money order.				
Capability	Provide ability to manage billing for retroactive enrollment.				

Capability	Provide capability for authorized users to adjust employer premium payment information to resolve discrepancy.				
Capability	Provide the ability to build and manage carrier plans, premiums, and tier information.				
Capability	Provide the capability for Agents / Brokers to view key data about their clients such as application status, employer plan selection status, status of employee enrollment.				
Capability	Provide ability to access all data for reporting.				
Capability	Provide ability for adhoc report creation.				
Capability	Provide ability to create user reports to manage support functions.				
Capability	Provide ability to upload documentation from batch or individual scan.				
Capability	Provide ability to receive documentation via web portal applications.				
Implementation	Provide training plan, resources, and implementation plan.				
Implementation	Provide training, training environment, and staff resources.				
Implementation	Provide integrated end-to-end testing, testing environment, and staff resources.				
Implementation	Provide support staff for issue resolution or on-site support				
Implementation	Provide post implementation support.				
Integration	Provide interfacing capability to receive data from, and send data to, Insurance Carriers.				
Integration	Provide interfacing capability to receive data from, and send data to, the CMS data HUB.				
Integration	Provide interfacing capability to receive data from, and send data to, Payment Processors.				
Integration	Provide interfacing capability to Oracle Identity Management.				
Integration	Provide interfacing capability to 3rd party adhoc reporting tools.				
Integration	Provide interfacing capability with Siebel and/or other CRM's.				
Services	Offer a Hosting solution as a service.				
Services	Offer call center capability as a service				
Services	Offer payment processing as a service				
Services	Offer individual/family exchange capability				
Services	Offer SaaS (Software as a service) as a solution.				
Services	Provide help center for product support.				

Appendix B:

Questions for States

Questions for Other States

1. *State-Based (SBM or SSBM) Exchange Using Federal Marketplace – general questions*

    - How much had your state invested in an SBM, if any, before you moved to the federal technology?
    - Did you do a gap analysis of your SBM?
        - How much did it cost?
        - How long did it take?
    - Is your Medicaid eligibility in a different system?
        - Did you do a gap analysis for Medicaid MAGI?
        - How much? How long?
    - Do you run your own SHOP or use healthcare.gov?
        - If running your own SHOP do you use the healthcare.gov infrastructure?
            - If using healthcare.gov infrastructure:
                - Do you use healthcare.gov for other related SHOP services such as eligibility, call center, payment processing? Other?
                - What are the cost for these services and how structured?
                - Were they willing to integrate, or modify their solution to accommodate your needs?
        - If running your own shop do you lease your SHOP solution?
                - What are the costs and how are they structured?
        - If using healthcare.gov for SHOP, are you using your own SBM for individual market eligibility and enrollment?

2. *Individual Market cost/operations issues*

    - Costs for carriers to establish interfaces with the FFM
        - What interfaces do they generally need?
    - Costs to the SBM for technology
        - SERFF to HIOS – did you incur costs from developing this?
    - Other costs – what else?

3. *Medicaid cost/operations issues*

    - Build interfaces for Minimum Essential Coverage and Account Transfers
        - Are there other IT modifications needed?
        - Did you automate these or use a manual system?
        - How much did it cost if automated? If manual?
    - How is this going? Did you have other costs?
    - Was your call center cost increased? How much? How has this trended over time?

4. *Other Costs?*

- Project management & transitional operations assistance
- Education and Outreach
- Call Center
    - Retraining
    - Operations issues?
- Payment Processing?
- Additional transition costs?

Appendix C:

State Exchange Interview Notes

State	Maryland	Nevada	Hawaii	Oregon
Individual Market Model - Current	SBM	SSBM	SSBM	SSBM
Model - Previous	SBM	SBM	SBM	SBM
Exchange Tech Vendor (May be different for Medicaid)	Systems Integrator: Deloitte. Bought technology from CT's vendor. Trying to share resources with CT, but that is not working very well & is not saving costs.	FFM technology	in process of moving to FFM technology now	FFM technology Required to run parallel systems for 15 months
Individual Market System Description	Bought CT's system with code freeze as of June 2014. Maryland has been responsible for finishing technology functions, including renewals, 1095 production, and dental. This is not an exhaustive list. Not sure if CT's tech has these functions now, so a state purchasing the code might be further along. Biggest technical problem was allowing people to start multiple applications, which has created a lot of customer service issues. Also, system sends 834s with any tiny change, which is inefficient and creating a lot of work for carriers as well. The system is not integrated with Medicaid, resulting in manual input of Medicaid applications.	Operated state technology for a year. Had lower (11,000) than expected (118,000) enrollment. Using fed technology for individual market; own SHOP. Built a prescreening tool for their informational website to direct people to Medicaid where eligible in order to minimize work arounds for lack of Medicaid integration. Also built in person assisters locator tool, because fed tool isn't very good. Paying to host this locator tool through Amazon gov't hosting site.	Moving to FFM technology now. Medicaid is using a pre-existing system for eligiblity - they already had an online portal and appropriate connections to the fed hub on citizenship & income verification. They had to build MEC & account transfers, so this was significantly less IT build than Oregon (for example).	Spent $300M on Oracle technology, which never went live. System is not integrated with Medicaid

Indiv Marketplace Tech Costs	$45M to date for both individual market & MAGI Medicaid. This is development costs, not M&O and hosting costs. No cost for CT code; paid CT for training on new system	$10M DDI to switch; total around $18M plus $7M to upgrade call center	$2 to $2.5M	Ongoing costs to maintain data for 7 years - $200-400,000/year; cost of decommissioning software not yet determined. Agreed to send budget, but it was not received as of filing this report.
Decommissioning Costs	Unknown.	Nevada reported costs of $27,544.28 for IRS data, including 2 software licenses for SQL Server softward, an SQL service, cable lock, and external CD reader. Presumably there are also staff who are able to compile the data if needed. It is unclear whether this is in compliance with CCIIO guidance, which also requires the ACA data to be archived and the Exchange software to be archived. Nevada reported needing to store 3 TB of data (Vermont's data, by comparison, is about 100TB of data).	Hawaii is procuring a data archival solution right now – the range of their bids is $3.5 to $7M, which includes a requirement to support the archive solution for 10 years.	Oregon came in with $1-5M as their bid range. They went with a $1M system by a vendor familiar with their system. For vendors who are unfamiliar with their system, their bids came in $3-5M range, because that vendor would need to learn the system. They estimate M&O on the archived data to be around $200,000.

SHOP Description	The state contracted with 3 big third party administrators to run their SHOP.	Nevada runs its own SHOP exchange.	In 2016, they are directly enrolling with Kaiser (the only carrier available). Only have 1000 people in SHOP. Don't know what they will do for 2017, except that they would prefer to get a 1332 waiver in order to maintain their employer mandate from the 1970s (predates ERISA preemption & they have a statutory exemption from ERISA).	Feds gave them a pass for 2015. They are using a paper process to determine small business tax credits. Not clear what they will do going forward. They have a policy issue related to their insurance rating (composite rates). They are exploring whether to make a state policy change to align with federal requirements in order to use FFM SHOP.

Medicaid Integration Description	Not integrated. System produced PDFs & Medicaid has to manually input the data into their system.	Originally tried state integration; but had to build new MAGI capabilities on old AHS Legacy system. Built Medicaid functions in 2 steps: 1) feds sent a PDF & state eligibility workers typed it into the state sytem; 2) automated transfer of information. Automated transfers is currently working well.	Not integrated	Bought Kentucky's IE solution because they needed to build Medicaid enrollment functions. They did need to make additional changes to implement. They had to build a public facing website, a fillable PDF application, account transfer & MEC capability, screen for eligibility so they did not send people to FFM who were not eligible for MAGI or exchange, and non-MAGI medicaid eligiblity (which they had intended to integrate into their exchange eligiblity system).
Medicaid Tech Costs	see below	$25M (90-10 match) to accept accounts and do MAGI eligibility (excludes rules engine, which was already built); news article quotes Damon Haycock as saying welfare spent $18M on DDI and $7M on call center	$10-20M	$62M (90-10 match), which includes $10M gap analysis of Oracle components for reusability; $3M for medicaid application/website re-development;$1M PMO; $40+M new licenses, DDI, etc

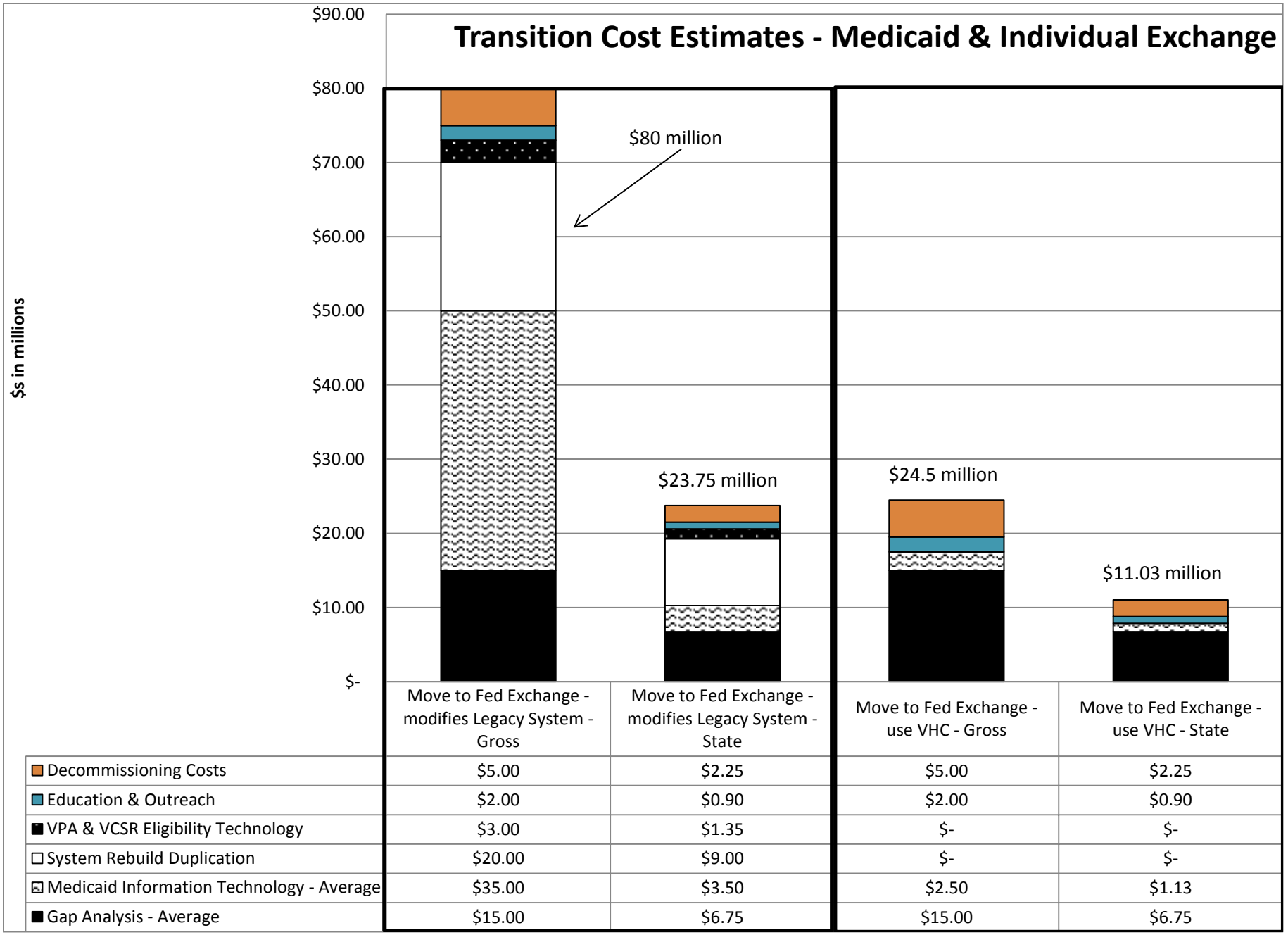
Gap Analysis Description	Analyzed options for moving from SBM to FFM, other state technology, brand new system from scratch. Determined it would cost $5-10M to connect to the Fed Technology, plus $40-50M to build Medicaid MAGI eligibility system. Buying CT's technology was $45M including Medicaid MAGI technology. In addition to tech gap analysis, Maryland had to do a Medicaid rules analysis in order to modify their state rules to be the same as CT's state rules.	CCIIO requires an options analysis. They looked at 1) fix their system - costs were unknown; 2) SBM using fed platform 3) Using the CT system - $50-60M; 4) FFM - free to the exchange, but there are still medicaid costs per above.	yes, IT work was minimal due to new Medicaid tech already in place.	Hired Deloitte to look at what they built for the exchange to see if anything was re-usable for Medicaid. See above cost estimate.
Gap Analysis Cost	unsure - part of larger analysis above	unsure	Unsure	Budgeted $18.4M, but spent about $10M
Amount spent pre-switch	$72M, settled lawsuit with original (fired) vendor for $45M	$50-60M total; $18M on Exchange DDI;	$120-130M	$300M

Identified current issues	Still doing DDI to fix things that didn't work well in CT technology when code was frozen.	Insufficient data & reporting from the FFM (no open enroll data in timely fashion); when customers have problem, state can advocate with the feds but cannot fix the problem. Work through the state officer, who is a liaison with the fed technology team & brings back information. This is bottlenecked & slow currently. No information on appeals.	Everyone has to re-enroll into FFM, which will be a difficult customer service challegne. In addition, the state will not have access to any data about individuals enrolled in coverage through FFM. Just beginning to build a PMO at the state level. HI has a lot of mixed families (parents in exhcange; kids on medicaid) & this will be a real customer service challenge.	KY code was transferred in. They needed to change some medicaid eligiblity rules but picked KY because rules were very similar to begin with. They had trouble with CMS data files for awhile - they didn't have anyone who could originally work with them & had to hire. IRS agreed to removal of FTI data, simplifying archival security and access requirements
Costs to carriers	unknown, but they didn't complain	unknown, but they did not complain. They have mostly nationwide carriers who had already built necessary interfaces &/or direct enrollment interface.	unknown, but mostly national carriers who had already connected to FFM in another state.	unknown, but they did not complain. Most carriers were national carriers so had already developed FFM connections for other states
Other costs		Project management - included in $10M above - about $2M; Education & Outreach - $2-3M effort because healthcare.gov will not do data transfers, so all people have to re-enroll into fed system.	$4M for navigators/assisters	Outreach & Ed - $1M, but didn't need a lot of outreach give that they didn't launch - lots of free bad press. Recommend planning for this if need to switch.

Call Center	Interviewee didn't have this information.	Not integrated with Medicaid call center. $300-400k per year. Downsize from 10 to 5 call center workers outside of open enrollment. Contracted with a navigator organization to run the call center. Can only facilitate, can't fix issues because they do not have access to the accounts.	Won't have access to federal accounts, so that will be a challenge for mixed households	created 400 temp positions to handle paper processing. Can't separate out costs separately.
Materials available?	Checking to see if can send us the gap analysis. Not received at the time this report was filed.	exchange.nv.gov/meetings/board/ May 2015 on		

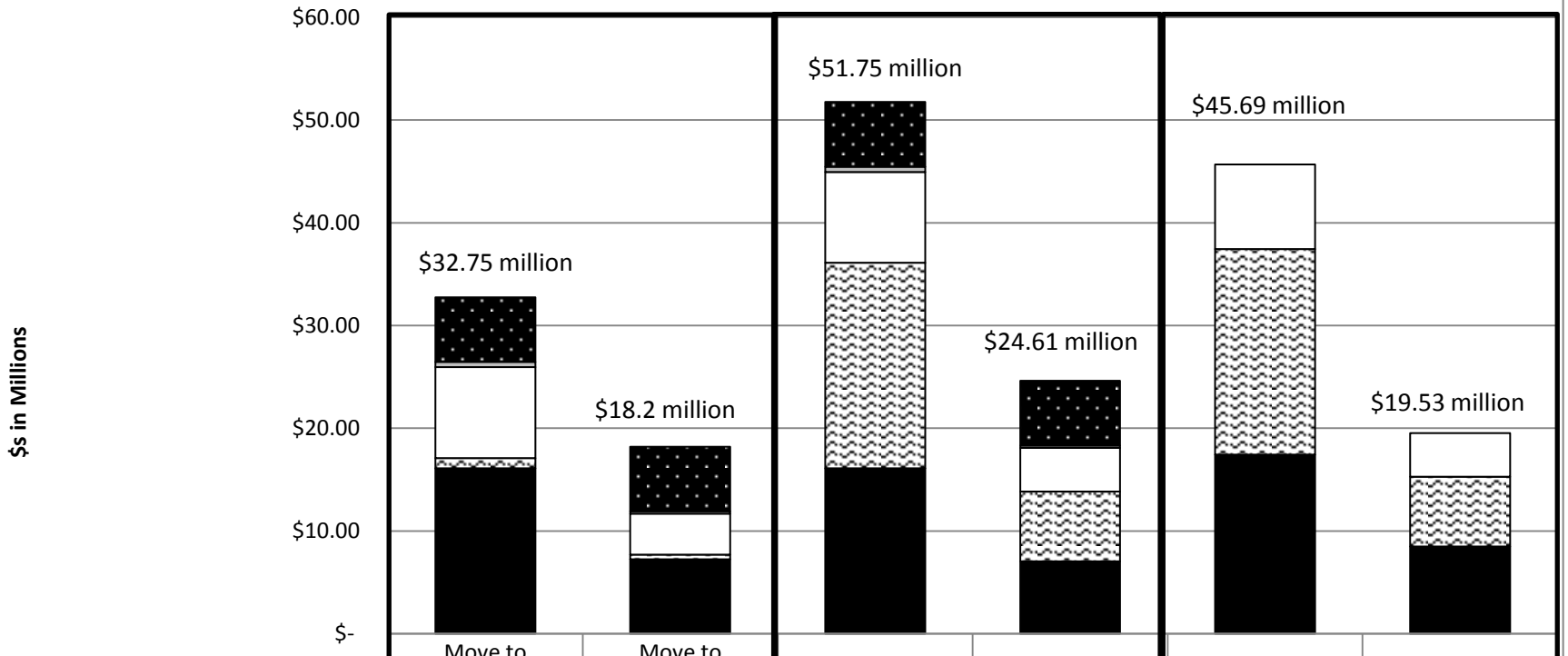
Appendix D:

VHC Cost Estimate Summaries



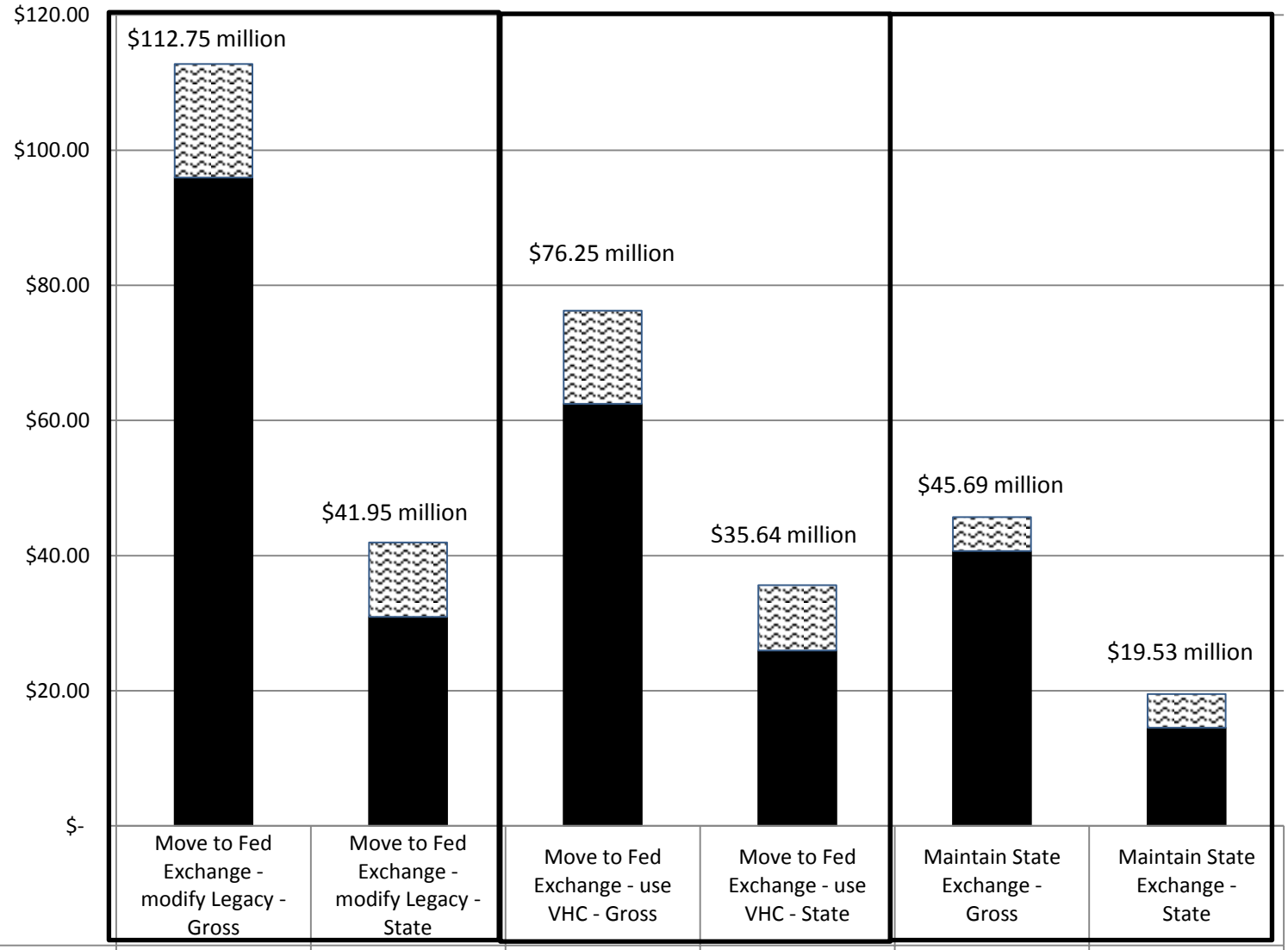
	Move to Fed Exchange - modifies Legacy System - Gross	Move to Fed Exchange - modifies Legacy System - State	Move to Fed Exchange - use VHC - Gross	Move to Fed Exchange - use VHC - State
Decommissioning Costs	$5.00	$2.25	$5.00	$2.25
Education & Outreach	$2.00	$0.90	$2.00	$0.90
VPA & VCSR Eligibility Technology	$3.00	$1.35	$-	$-
System Rebuild Duplication	$20.00	$9.00	$-	$-
Medicaid Information Technology - Average	$35.00	$3.50	$2.50	$1.13
Gap Analysis - Average	$15.00	$6.75	$15.00	$6.75

Ongoing Costs: Medicaid & Individual Exchange

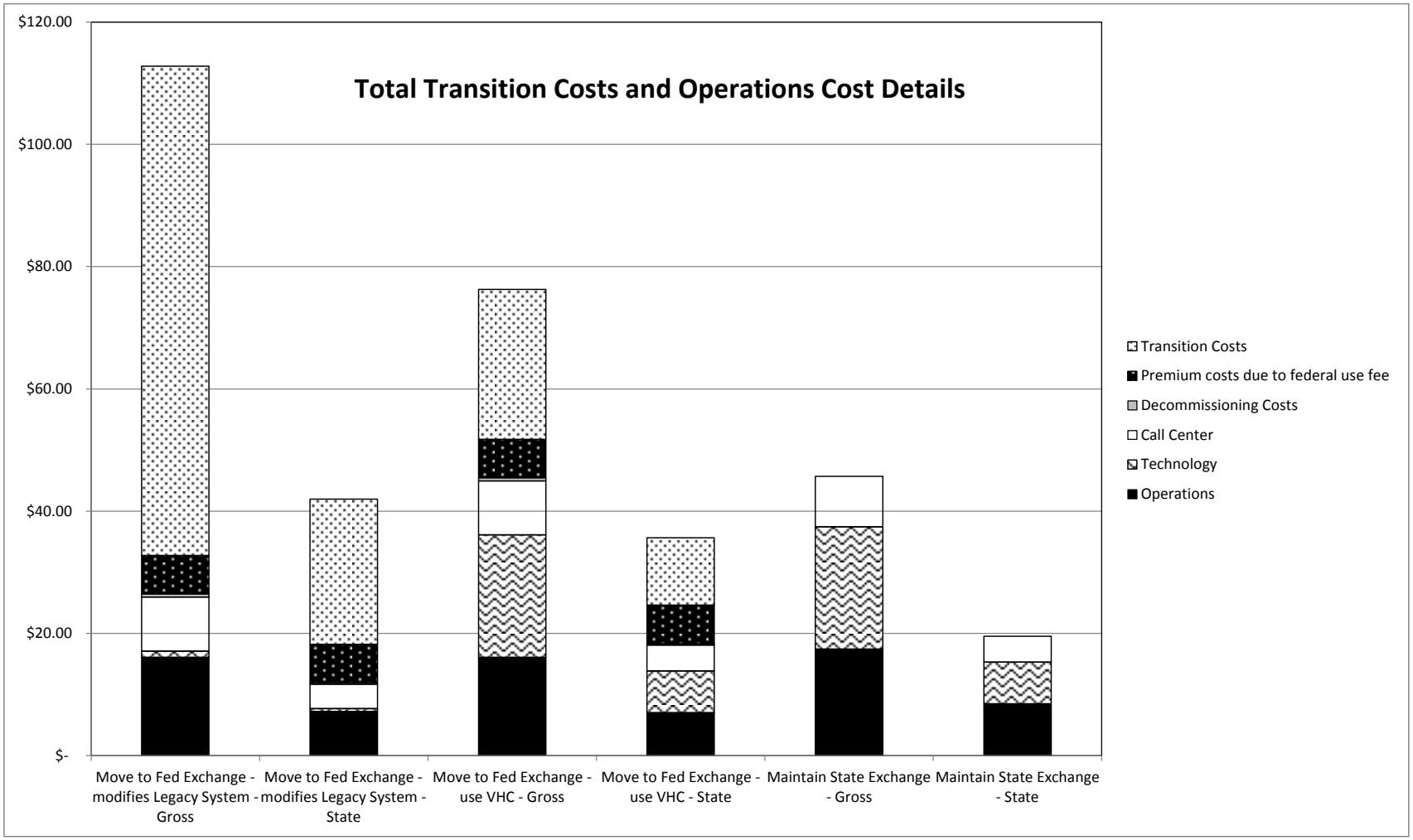


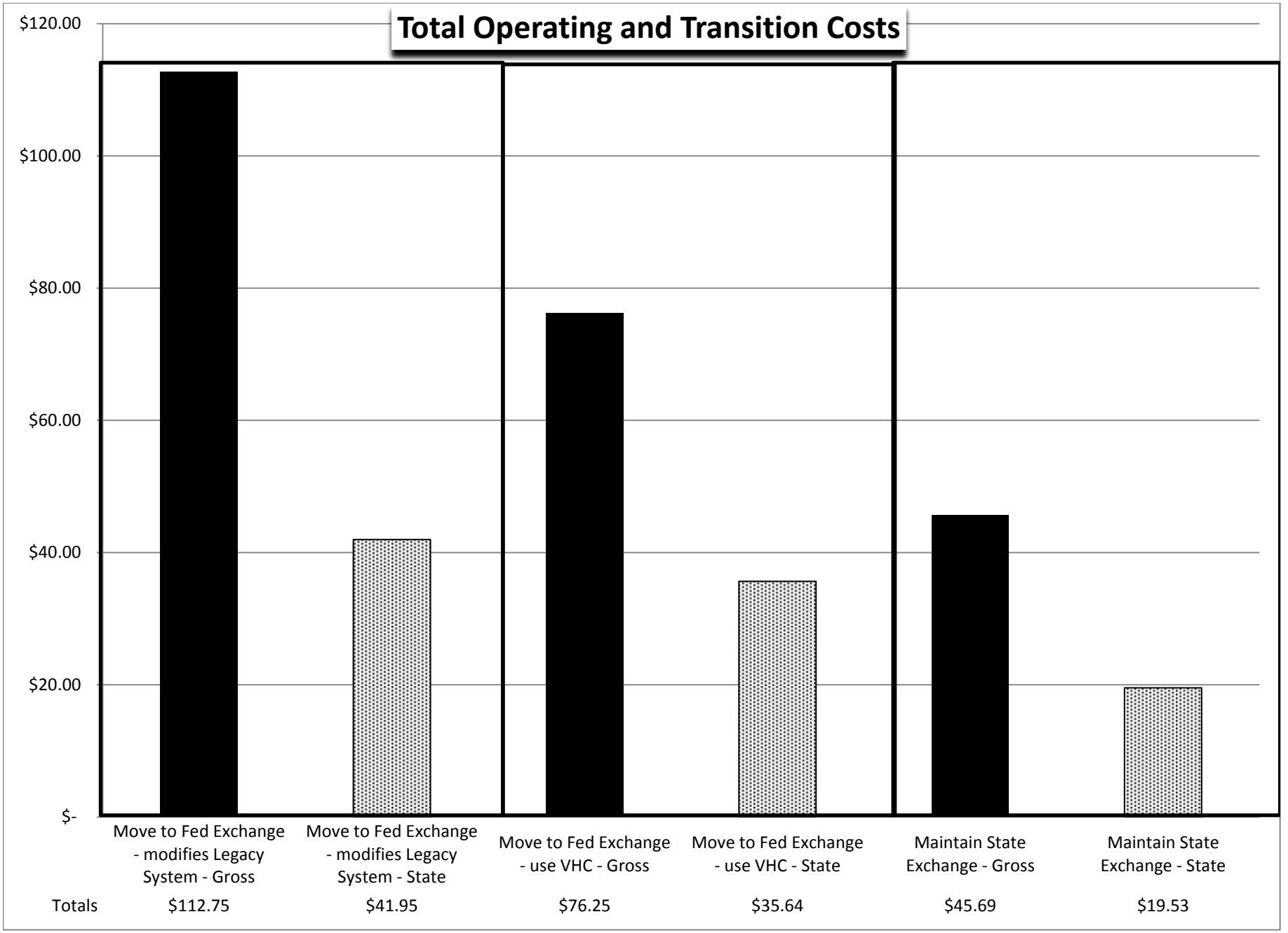
	Move to Fed Exchange - modifies Legacy System - Gross	Move to Fed Exchange - modifies Legacy System - State	Move to Fed Exchange - use VHC - Gross	Move to Fed Exchange - use VHC - State	Maintain State Exchange - Gross	Maintain State Exchange - State
Premium costs due to federal use fee	$6.30	$6.30	$6.30	$6.30	$-	$-
Decommissioning Costs	$0.50	$0.23	$0.50	$0.23	$-	$-
Call Center	$8.85	$3.98	$8.85	$4.25	$8.25	$4.25
Technology	$1.00	$0.45	$20.00	$6.78	$20.00	$6.78
Operations	$16.10	$7.25	$16.10	$7.05	$17.44	$8.49

Total Costs: Medicaid and Individual Exchange



	Move to Fed Exchange - modify Legacy - Gross	Move to Fed Exchange - modify Legacy - State	Move to Fed Exchange - use VHC - Gross	Move to Fed Exchange - use VHC - State	Maintain State Exchange - Gross	Maintain State Exchange - State
Costs to the Exchange	$16.80	$11.03	$13.80	$9.68	$5.00	$5.00
Costs to Medicaid	$95.95	$30.93	$62.45	$25.96	$40.69	$14.53


Total Transition Costs and Operations Cost Details
$120.00
$100.00
$80.00
$60.00
$40.00
$20.00
$-
Move to Fed Exchange - modifies Legacy System - Gross
Move to Fed Exchange - modifies Legacy System - State
Move to Fed Exchange - use VHC - Gross
Move to Fed Exchange - use VHC - State
Maintain State Exchange - Gross
Maintain State Exchange - State
Transition Costs
Premium costs due to federal use fee
Decommissioning Costs
Call Center
Technology
Operations


Total Operating and Transition Costs
$120.00
$100.00
$80.00
$60.00
$40.00
$20.00
$-
Move to Fed Exchange - modifies Legacy System - Gross
Move to Fed Exchange - modifies Legacy System - State
Move to Fed Exchange - use VHC - Gross
Move to Fed Exchange - use VHC - State
Maintain State Exchange - Gross
Maintain State Exchange - State
Totals
$112.75
$41.95
$76.25
$35.64
$45.69
$19.53

Medicaid & Individual Exchange (does not include Small Business Exchange Cost Estimates)

Total Costs	SSBM (no reuse of VHC; modifies ACCESS) to Fed Exchange - modify Legacy	to Fed Exchange - modify Legacy	SSBM using VHC ve to Fed Exchange - use VHC - G	ve to Fed Exchange - use VHC - St	Maintain VHC Maintain State Exchange - Gross	Maintain State Exchange - State	Comments
Costs to the Exchange	$ 16.80	$ 11.03	$ 13.80	$ 9.68	$ 5.00	$ 5.00	Maintain State Exchange is the SFY'18 Sustainability Budget
Costs to Medicaid	$ 95.95	$ 30.93	$ 62.45	$ 25.96	$ 40.69	$ 14.53	
Total	$ 112.75	$ 41.95	$ 76.25	$ 35.64	$ 45.69	$ 19.53	

Transition Chart Data	Move to Federal Exchange - modifies ACCESS) d Exchange - modifies Legacy Sys	d Exchange - modifies Legacy Sys	SSBM using VHC ve to Fed Exchange - use VHC - G	ve to Fed Exchange - use VHC - State	
Gap Analysis - Average	$ 15.00	$ 6.75	$ 15.00	$ 6.75	Based on an average of other states. At GC match rate (55/45).
Medicaid Information Technology - Average	$ 35.00	$ 3.50	$ 2.50	$ 1.13	Based on an average of other states. At enhanced rate (90/10).
System Rebuild Duplication	$ 20.00	$ 9.00	$ -	$ -	Based on average of other states. Assumes modern tech won't cost as much for rebuild. At GC match rate (55/45).
VPA & VCSR Eligibility Technology	$ 3.00	$ 1.35	$ -	$ -	Based on DCF's estimates to add subsidy programs. At GC match rate (55/45).
Education & Outreach	$ 2.00	$ 0.90	$ 2.00	$ 0.90	Based on actual experience when building VHC. At GC match rate (55/45)
Decommissioning Costs	$ 5.00	$ 2.25	$ 5.00	$ 2.25	Based on average of other states. At GC match rate (55/45).
Total	$ 80.00	$ 23.75	$ 24.50	$ 11.03	

Ongoing Costs Chart Data	Move to Federal Exchange - modifies ACCESS) d Exchange - modifies Legacy Sys	d Exchange - modifies Legacy Sys	SSBM using VHC ve to Fed Exchange - use VHC - G	ve to Fed Exchange - use VHC - St	Maintain State Exchange - Gross	Maintain State Exchange - State	
Technology	$ 1.00	$ 0.45	$ 20.00	$ 6.78	$ 20.00	$ 6.78	Based on current sustainability budget for VHC; reduced growth built in by approx 3% to reflect current year. Reflec
Operations	$ 16.10	$ 7.25	$ 16.10	$ 7.05	$ 17.44	$ 8.49	Based on current sustainability budget for VHC; reduced growth approx 3%. Reflects OAPD funding.
Call Center	$ 8.85	$ 3.98	$ 8.85	$ 4.25	$ 8.25	$ 4.25	Based on current sustainability budget for VHC; reduced growth approx 3%. Reflects OAPD funding.
Premium costs due to federal use fee	$ 6.30	$ 6.30	$ 6.30	$ 6.30	$ -	$ -	$180 Million base - 2.8% 100% state funding.
Decommissioning Costs	$ 0.50	$ 0.23	$ 0.50	$ 0.23	$ -	$ -	Based on average of other states. At GC match rate (55/45). Required for 10 years.

Appendix E:

CMS IT Decommissioning Data Retention Planning

SBM IT Decommissioning Data Retention Planning

Appendix A

State-based Marketplace (SBM) IT Decommissioning and Data Retention Planning

Contents

PURPOSE AND OVERVIEW

This document provides a list of required actions for states that are decommissioning components of their Marketplaces, or the entire Marketplace, and that may transition to the Federally-facilitated Marketplace (FFM) system. The actions described in this document are required in the following situations, a Marketplace decides to: 1) replace the entire Marketplace IT system; 2) replace any component(s) of the Marketplace IT system(s); 3) change Marketplace models and migrate IT system functions to the FFM IT system; or 4) change Marketplace IT support vendors or other key contractor support personnel. Decommissioning plans apply both in cases where the state intends a permanent or temporary closure of its Marketplace IT.

The technical assistance in the document is consistent with federal government Capital Planning and Investment Control practices (CPIC), specifically the Disposition/Decommissioning phase of an IT investment, as is required by Office of Management and Budget (OMB) Circular NO. A-130, Revised, Management of Federal Information Resources, Nov 2000. This technical assistance is also consistent with practices employed by the Department of Health and Human Services (HHS) and Centers for Medicare & Medicaid Services (CMS), in their effort to monitor IT system development through formal system development lifecycle activities. The document references applicable federal laws, regulations and guidance related to the disposition and/or decommissioning of IT systems, or as necessary, the preservation and/or destruction of Marketplace data.

These IT decommissioning, data retention and data disposition activities ensure the orderly decommissioning of the Marketplace IT systems and the preservation of vital information about the system, so that some or all of the Marketplace information may be reactivated immediately or in the future. Particular emphasis is given to proper preservation of the data processed by the system, so that the data is effectively migrated to another system or archived in accordance with applicable records management regulations and policies for potential future access (see 45 CFR §155.1210 Maintenance of Records). Equipment must be sanitized to ensure the data is not comprised or misused, particularly with regard to personally identifiable information (PII) or other types of protected information.

APPLICABLE LAWS, REGULATIONS, STANDARDS, AND AGREEMENTS

The following list of laws, regulations, funding opportunity announcements (FOAs) and other guidance documents include applicable records and data retention, recovery, protection, and destruction requirements and is provided here as a reference, however the list is not all inclusive:

- The Patient Protection and Affordable Care Act of 2010, (Pub. L. 111-148) as amended by the Health Care and Education Reconciliation Act of 2010 (Pub. L. 111-152).
- 45 CFR Parts 155, 156, and 157 Patient Protection and Affordable Care Act; Establishment of Exchanges and Qualified Health Plans; Exchange Standards for Employers including; § 155.260, *Privacy and security of personally identifiable information* and § 155.280 *Oversight and monitoring of privacy and security requirements*.
- Internal Revenue Service Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies, Jan 2014.
- E-Government Act of 2002, (Pub. L. 107–347) 44 U.S.C. § 101
    - E-Government Act of 2002, Privacy requirements including the Privacy Impact Assessment, 44 U.S.C § 3501, Sec. 208.
- The Privacy Act of 1974 (Pub. L. 93–579) as amended, (5 U.S.C. § 552a).

- SBMs that connect to the Federal Data Services Hub (FDSH) must sign the:
    - Interconnection Security Agreement (ISA).
    - Computer Matching Agreement (CMA).
    - Information Exchange Agreement (IEA).
- CMS Minimum Acceptable Risk Standards for Exchanges (MARS-E) Document Suite.
- National Institutes of Standards and Technology (NIST) Special Publications (SP) such as:
    - SP 800-88 Revision 1 (draft), Guidelines for Media Sanitization, September 2012.
    - SP 800-147, BIOS Protection Guidelines, April 2011.
    - SP 800-160 Initial Public Draft System Security Engineering An Integrated Approach to Building Trustworthy Resilient Systems (Section 3.11)

Office of Management and Budget (OMB) Circular NO. A-130, Revised, Management of Federal Information Resources, Nov 2000.

The primary system transition, decommission and data mitigation activities are described in greater detail in the remainder of this document. This document primarily describes activities that will require considerable involvement by states, including the submission of action plans, activities, and other relevant information to CMS. If any step is not applicable or cannot be completed, the rationale must still be documented and submitted to CMS for review. CMS will evaluate the information submitted by states, approve or disapprove, and require updates accordingly before execution of planned activities are allowed to be conducted.

MARKETPLACE IT SYSTEMS AND DATA MIGRATION ACTIVITIES

Table 1: IT Systems and Data Migration Activities

Task	Task Name	Description
1	Overall Migration Plan	• Describe the business functions from the Marketplace IT system that will be supported by the FFM. Discuss the type of data (e.g., information classes/data subject areas) maintained in the Marketplace IT system that will be migrated to be included in the FFM. • Describe the Marketplace IT system structure and major components and designate which system components will and will not be migrated. If the migration process will be organized into discrete phases, identify which system components will undergo migration in each phase. Address in explicit subsections the migration overview associated with hardware, software, and data, as appropriate. • Work with CMS to define the data migration strategy, data quality assurance, and data migration controls. Describe how data will be migrated, measured, and secured; the controls that will be in place to ensure that data migration has been successful; and any requirements associated with maintaining/transferring authoritative data source (ADS) designations or related service-level agreements (SLA). Describe the major risk factors in the data migration effort and strategies for their control or reduction. • Describe efforts to maintain the confidentiality, integrity, and availability of sensitive data (i.e., personally identifiable information or tax information) currently hosted in the system to be

		decommissioned until it is verified as destroyed and not retrievable.
1.1	Hardware and Software Migration	Work with CMS to define an overall strategy and activities required needed for the migration from Marketplace IT system hardware and software to the FFM. List and describe the Marketplace hardware and software that will continue to be used and will no longer be used.
1.2	Data Migration Requirements	Work with CMS to define the specific data preparation requirements and the Marketplace data that must be available for the migration. If data will be transported from the original Marketplace IT system, work with CMS to define a detailed description of data handling, migration, and loading procedures. If the data will be transported using machine-readable media, describe the characteristics of each media component.
1.3	Data Migration Mapping	List and account for all data mapped to the Marketplace IT system in terms of where and when it will be migrated.
1.4	Data Migration Security Requirements	• Work with CMS to define security requirements for establishing connections between the state Marketplace IT system and the FFM when migrating data. • Work with CMS to outline data security and associated risk mitigation strategies. Identify the impacts to Marketplace IT and/or the FFM during the data migration and develop a strategy for mitigating the risks. Specifically, identify what security controls will be implemented during the migration process, for example: o Access controls: Access to/responsibility for the data during the entire process is documented. o Configuration management: Validated effective and operational functions maintain data integrity. o Change management: Documented process for requesting, approving, and implementing changes to IT systems and supporting operational processes as it specifically applies to the FFM data migration. o Contingency planning: An exact copy of data is maintained during the migration process in case of a failure. o Identification and authentication: All hardware is authenticated before the migration process is initiated. Encryption is implemented for data transmission. o Planning: System Security Plan is updated as components of the Marketplace IT system are decommissioned. o Risk management: Mitigation plans are documented and implemented to address known and potential risks/vulnerabilities during the migration process. o Media sanitization: Hardware is tested to ensure data is destroyed and not retrievable. o Privacy impact assessment (PIA): The PIA is updated and validated.
1.5	Legal Agreements	Coordinate with CMS to establish a memorandum of understanding (MOU), or similar legal agreement, to document data migration security requirements.
1.6	Impact to Other	Describe the state Marketplace IT system's interfaces to other state,

	System Interfaces	issuer, Federal, and agency systems that will be affected by the data migration. List each affected interface and the necessary changes to support or eliminate the interface upon migration.
1.7	Test Plan	Work with CMS to define the testing that will be conducted to ensure that all migration activities are successful. At a minimum, include who will perform the testing, the test cases that will be performed, and how the results of the testing will be tracked and reported.
1.8	Migration Schedule	Create a work breakdown schedule (WBS) consisting of activities, tasks, milestones, and a fully developed test plan. Identify critical design reviews, indicating progress of the migration itself.
1.9	Migration Resources	Describe the state resources necessary to perform the migration. Highlight required hardware, software, people, and facility resources not currently available and detail an approach for obtaining all currently unavailable resources.
1.10	Administrative Responsibilities	• Describe the process and the steps taken to ensure all old legal contracts and agreements (including service-level agreements) have been closed and nullified. • Describe the process and the steps taken to implement new agreements, as required, including roles and responsibilities for signatures and approvals.

Perform Migration Activities

All documentation included in Table 1 must be submitted to CMS for approval before any migration activities can occur. The migration should be performed based on the approved migration plan in Table 1. This step should not be initiated until the necessary migration resources outlined in the plan are available and risks have been accepted or mitigated. At the end of the migration, the state project manager will coordinate management approvals of documentation created during the activity. Management approval and acknowledgement will be formally documented and the final documentation must be submitted to CMS.

MARKETPLACE IT SYSTEMS AND DATA DECOMMISSION ACTIVITIES

All activities involved in the establishment and execution of the state Marketplace IT system decommission are listed below. The first decommissioning activity is the development of a decommission plan for the Marketplace IT system. Upload all decommissioning artifacts into CALT.

Table 2: IT Systems and Data Decommission Activities

Task	Task Name	Description
2	Marketplace IT Decommission Plan	Work with CMS to develop the decommission plan. The decommission plan ensures the decommissioning of the Marketplace IT system is planned and executed in a way that data and application logic are preserved, affected parties are appropriately notified, and disposition of hardware and software is conducted in compliance with established state and Federal guidelines. The remaining tasks within this table describe the various tasks required for the system decommission.

2.1	Software Archival	Describe the activities for archiving the software library files and related documentation in the system being decommissioned, including which software will be archived, and in which format. The intent of the software archive is to provide sufficient stored software so the system could be re-initiated if necessary.
2.2	Documentation Archival	Describe the activities for archiving the hard copy and soft copy user documentation for the Marketplace IT, including which documentation will be archived and in which format. The intent of the documentation storage is to provide sufficient archived documentation so the system could be re-initiated and used if necessary.
2.3	Hardware Disposition	Describe the activities for disposing of hardware that was used exclusively by the state Marketplace IT system, including the methodology for ensuring data cannot be retrieved from the decommissioned equipment.
2.4	Data Retention and Destruction	Describe the activities for retaining data files and related documentation of the system being decommissioned and the length of that retention period. Outline which data have been migrated, which data will be retained, and in which format, and which data will be destroyed. 45 CFR §155.1210 Maintenance of Records, states the SBMs must maintain and ensure its contractors, subcontractors, and agents maintain certain documents and records for ten years. These documents and records (whether paper, electronic, or other media) and other evidence of accounting procedures and practices, must be sufficient to: accommodate periodic auditing of financial records, and enable the US Department of Health and Human Services (HHS) or its designee(s) to inspect facilities, or otherwise evaluate the SBM's compliance with Federal standards.
2.5	Legal Agreements, System Security Plan, and Associated Artifacts	• Coordinate with CMS to update legal agreements established between CMS and the state to allow connection to the FDSH. States may need to change the state signatory on the legal agreements. • Update and retain the system security plan (SSP), which should describe the system security and access rights associated with the Marketplace IT system. The SSP should describe the necessary security information so the system could be reconstituted with the same security considerations, if necessary. • Update the IRS Safeguard Security Report and submit to IRS at safeguardreports@irs.gov. This report is the primary source for the state to report to IRS on the processes, procedures, and security controls in place to protect Federal Tax Information (FTI) and must be submitted annually in accordance with IRC 6103(p)(4), as long as FTI is retained. Additionally, the state may not transfer the custody of FTI to another state agency (or vendor) before notification and approval of the IRS.
2.6	Decommission Schedule	Provide a WBS that consists of the activities, tasks, milestones, and review points for the decommission itself.
2.7	Decommission Resources	Describe the state resources necessary to perform the decommission activities, including identification of required hardware, software, people, and facility resources and a detailed approach for obtaining all currently

		unavailable resources.

Perform Decommission Activities

All documentation included in Table 2 must be submitted to CMS for approval before any decommission activities can occur. The system decommission should be performed based on the approved decommission plan. This step should not be initiated until the necessary decommissioning resources outlined in the plan are available and risks have been accepted, eliminated, or mitigated. At the end of the decommission process, the state project manager will coordinate management approvals of documentation created during the activity. Management approval and acknowledgement must be formally documented and the final documentation must be submitted to CMS.

STATE-BASED MARKETPLACE IT DECOMMISSIONING AND DATA RETENTION FREQUENTLY ASKED QUESTIONS

1. WHAT ARE THE CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS) OR "OTHER" REQUIREMENTS WHEN A STATE-BASED MARKETPLACE (SBM), OR COMPONENT(S) OF AN SBM, IS BEING DECOMMISSIONED? PLEASE INCLUDE REQUIREMENTS FOR RETENTION, RECOVERY, PROTECTION, AND DESTRUCTION.

The requirements for decommissioning a Marketplace information technology (IT) system, or components of the system, can be found in Federal regulations, legal agreements, Funding Opportunity Announcements (FOAs), and other guidance documents applicable to SBMs. The requirements address records and data retention, recovery, protection, and destruction. Please reference CMS technical assistance materials and guidance on the CMS website under the XLC Process Overview site and associated pages, or ask your Center for Consumer Information and Insurance Oversight (CCIIO) State Officer or Office of Information Services (OIS) Information Technology (IT) Project Manager (PM) for additional information.

If an SBM is decommissioning Marketplace IT functionality as part of a Marketplace transition then the SBM must adhere to the requirements at 45 CFR §155.106 (b), *Transition process for State Exchanges that cease operations*. The requirements at 45 CFR §155.106 (b) state, "A State that ceases operations of its Exchange after January 1, 2014 must: (1) Notify HHS that it will no longer operate an Exchange at least 12 months prior to ceasing operations; and (2) Coordinate with HHS on a transition plan to be developed jointly between HHS and the State."

45 CFR §155.1210 Maintenance of Records, states the SBMs must maintain and ensure its contractors, subcontractors, and agents maintain certain documents and records for ten years. These documents and records (whether paper, electronic, or other media) and other evidence of accounting procedures and practices, must be sufficient to: accommodate periodic auditing of financial records, and enable the US Department of Health and Human Services (HHS) or its designee(s) to inspect facilities, or otherwise evaluate the SBM's compliance with Federal standards. The requirement further states that the records include, at a minimum, the following:

- Information concerning management and operation of the SBM's financial and other record keeping systems
- Financial statements
- Any financial reports filed with other Federal programs or State authorities
- Data and records relating to the SBM's eligibility verifications and determinations, enrollment transactions, appeals, and plan variation certifications
- Qualified health plan contracting (including benefit review) data and consumer outreach and Navigator grant oversight information.

SBMs must document a record and data retention schedule. SBMs that decommission a Marketplace information technology (IT) system, or components of the system, must update the record and data retention schedule to identify the records and data that must be retained and destroyed. The SBM must maintain records described in §155.1210 for ten years. Other Federal or state laws or regulations may require, or allow, data within this record set to be destroyed earlier than the retention period required by §155.1210. SBMs must adhere to the most stringent record retention timeframes.

An SBM must make all retained and archived records available and must ensure its contractors, subcontractors, and agents make all records available to HHS, the Office of the Inspector General (OIG), the Comptroller General, or their designees, upon request.

The following list of Federal regulations, legal agreements, FOAs and other guidance documents include applicable records and data retention, recovery, protection, and destruction requirements and is provided here as a reference, however the list is not all inclusive:

- The Patient Protection and Affordable Care Act of 2010, (Pub. L. 111-148) as amended by the Health Care and Education Reconciliation Act of 2010 (Pub. L. 111-152).
- 45 CFR Parts 155, 156, and 157 Patient Protection and Affordable Care Act; Establishment of Exchanges and Qualified Health Plans; Exchange Standards for Employers including; § 155.260, *Privacy and security of personally identifiable information* and § 155.280 *Oversight and monitoring of privacy and security requirements*.
- Internal Revenue Service Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies, Jan 2014.
- E-Government Act of 2002, (Pub. L. 107–347) 44 U.S.C. § 101
    - E-Government Act of 2002, Privacy requirements including the Privacy Impact Assessment, 44 U.S.C § 3501, Sec. 208.
- The Privacy Act of 1974 (Pub. L. 93–579) as amended, (5 U.S.C. § 552a).
- SBMs that connect to the Federal Data Services Hub (FDSH) must sign the:
    - Interconnection Security Agreement (ISA).
    - Computer Matching Agreement (CMA).
    - Information Exchange Agreement (IEA).
- CMS Minimum Acceptable Risk Standards for Exchanges (MARS-E) Document Suite.
- National Institutes of Standards and Technology (NIST) Special Publications (SP) such as:
    - SP 800-88 Revision 1 (draft), Guidelines for Media Sanitization, September 2012.
    - SP 800-147, BIOS Protection Guidelines, April 2011.
    - SP 800-160 Initial Public Draft System Security Engineering An Integrated Approach to Building Trustworthy Resilient Systems (Section 3.11)
- Office of Management and Budget (OMB) Circular NO. A-130, Revised, Management of Federal Information Resources, Nov 2000.

2. IS A STATE THAT TRANSITIONS FROM AN SBM TO ANOTHER MARKETPLACE MODEL REQUIRED TO ADHERE TO THE MINIMUM ACCEPTABLE RISK STANDARDS FOR EXCHANGES (MARS-E) REQUIREMENTS?

Yes, state Administering Entities (AE) that sign agreements with CMS to use data from the FDSH are required to adhere to the CMS MARS-E document suite. The state AE is required to adhere to records management, retention, and destruction requirements in regulations and agreements during and after the transition from an SBM to another Marketplace model. The state AE must continue to adhere to the MARS-E requirements while decommissioning the SBM IT system, or components of the IT system. The state AE that is responsible for the new Marketplace model must adhere to the MARS-E requirements while establishing a connection to the FDSH.

3. WHAT ARE THE REQUIREMENTS FOR DESTRUCTION OF MARKETPLACE DATA FOLLOWING THE IMPLEMENTATION OF A NEW MARKETPLACE MODEL?

All SBM documentation, records, and data subject to retention requirements must be securely stored for the duration of the Federal and/or state-defined retention periods. The SBM must maintain records described in §155.1210 for ten years. After the retention period, all personally identifiable information (PII) must be securely destroyed or disposed of in an appropriate and reasonable manner[1] as defined in the Marketplace regulations.

States that transition to a new Marketplace model are required to sign an attestation statement that all documentation, records, and/or data are properly retained or were destroyed in accordance with the Federal and state regulations and SBM policy and procedures. This includes restricting and limiting access to the records being retained.

The SBM must select and document appropriate and reasonable data destruction and disposal methods. This includes the disposal or sanitization of all system infrastructure components used for processing or storing media when no longer required. SBMs are required to document retention and disposal policy and procedures for all records, information, and media. The associated controls must be documented in the System Security Plan (SSP)[2]. The retention and destruction policy and procedures must address requirements defined in applicable Federal and state laws, regulations, legal agreements, FOAs, and other guidance documents. For example, states may reference guidance in National Institute of Standards and Technology (NIST) draft Special Publication 800-88 Revision 1, *Guidelines for Media Sanitization* and incorporate components of the guidance into their policy and procedures.

States that plan to temporarily transition to the Federally-facilitated Marketplace (FFM) but plan to reopen their Marketplace in the future should work with CMS to determine: whether certain data sets can be securely retained for future use. The state must work with CMS to determine the security requirements for the system storing the records and data (e.g., such as updated SSP, quarterly plan of action and milestones submissions and annual attestations).

4. WHAT ARE CMS' DATA ACCESSIBILITY REQUIREMENTS FOR DECOMMISSIONED SYSTEMS?

An SBM must maintain and must ensure its contractors, subcontractors, and agents maintain for ten years, documents and records (whether paper, electronic, or other media) and other evidence of accounting procedures and practices. See §155.1210 Maintenance of Records. The records and data must be securely stored on media that allows the state to make the data available and accessible to both individuals that are the subject of the data set and to Federal or state entities authorized by law to access the records or data. As a general rule an SBM should comply with the most stringent set of applicable requirements and never dispose of data while new guidance, litigation, an audit, or other form of investigation is occurring or is anticipated in the foreseeable future.

---

[1] See § 155.260 (a)(4)(vi).

[2] See Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement, Version 1.0, August 1, 2012; controls Media Protection, MP-6: Media Sanitization and all associated control enhancements; and System and Information Integrity, SI-12: Information Output Handling and Retention

5. DOES A STATE NEED TO SIGN NEW LEGAL AGREEMENTS WITH CMS WHEN TRANSITIONING TO A NEW MARKETPLACE MODEL?

This depends on the connection within the state to the FDSH. States entities must work with CMS to determine if modified or new agreements are required.

If an SBM is no longer operating a Marketplace IT system and does not solicit, accept, or transmit any PII or protected health information (PHI) then the legal agreements between CMS and the SBM will need to be transferred to the state entity that will obtain data from the FDSH. The SBM must continue to adhere to records and data retention requirements for all data obtained prior to the Marketplace model transition. The state must continue to work with the Internal Revenue Service to address safeguard requirements for Federal Tax Information.

SBMs that are transitioning to a new Marketplace model should review the *Privacy and Security Timelines and Artifacts For Health Insurance Marketplaces, Medicaid/CHIP Agencies and Partner Organizations* document (CALT ID: doc28905) for more information on legal agreements required when connecting to the FDSH.

6. WHAT IF I HAVE MORE QUESTIONS?

Please email your assigned State Officer and Jay Streit (jay.streit@cms.hhs.gov) if you have additional questions.

State-based Marketplace (SBM) IT Decommissioning and Data Retention Planning

Contents

PURPOSE AND OVERVIEW

This document provides a list of required actions for states that are decommissioning components of their Marketplaces, or the entire Marketplace, and that may transition to the Federally-facilitated Marketplace (FFM) system. The actions described in this document are required in the following situations, a Marketplace decides to: 1) replace the entire Marketplace IT system; 2) replace any component(s) of the Marketplace IT system(s); 3) change Marketplace models and migrate IT system functions to the FFM IT system; or 4) change Marketplace IT support vendors or other key contractor support personnel. Decommissioning plans apply both in cases where the state intends a permanent or temporary closure of its Marketplace IT.

The technical assistance in the document is consistent with federal government Capital Planning and Investment Control practices (CPIC), specifically the Disposition/Decommissioning phase of an IT investment, as is required by Office of Management and Budget (OMB) Circular NO. A-130, Revised, Management of Federal Information Resources, Nov 2000. This technical assistance is also consistent with practices employed by the Department of Health and Human Services (HHS) and Centers for Medicare & Medicaid Services (CMS), in their effort to monitor IT system development through formal system development lifecycle activities. The document references applicable federal laws, regulations and guidance related to the disposition and/or decommissioning of IT systems, or as necessary, the preservation and/or destruction of Marketplace data.

These IT decommissioning, data retention and data disposition activities ensure the orderly decommissioning of the Marketplace IT systems and the preservation of vital information about the system, so that some or all of the Marketplace information may be reactivated immediately or in the future. Particular emphasis is given to proper preservation of the data processed by the system, so that the data is effectively migrated to another system or archived in accordance with applicable records management regulations and policies for potential future access (see 45 CFR §155.1210 Maintenance of Records). Equipment must be sanitized to ensure the data is not comprised or misused, particularly with regard to personally identifiable information (PII) or other types of protected information.

APPLICABLE LAWS, REGULATIONS, STANDARDS, AND AGREEMENTS

The following list of laws, regulations, funding opportunity announcements (FOAs) and other guidance documents include applicable records and data retention, recovery, protection, and destruction requirements and is provided here as a reference, however the list is not all inclusive:

- The Patient Protection and Affordable Care Act of 2010, (Pub. L. 111-148) as amended by the Health Care and Education Reconciliation Act of 2010 (Pub. L. 111-152).
- 45 CFR Parts 155, 156, and 157 Patient Protection and Affordable Care Act; Establishment of Exchanges and Qualified Health Plans; Exchange Standards for Employers including; § 155.260, *Privacy and security of personally identifiable information* and § 155.280 *Oversight and monitoring of privacy and security requirements*.
- Internal Revenue Service Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies, Jan 2014.
- E-Government Act of 2002, (Pub. L. 107–347) 44 U.S.C. § 101
    - E-Government Act of 2002, Privacy requirements including the Privacy Impact Assessment, 44 U.S.C § 3501, Sec. 208.
- The Privacy Act of 1974 (Pub. L. 93–579) as amended, (5 U.S.C. § 552a).

- SBMs that connect to the Federal Data Services Hub (FDSH) must sign the:
    - Interconnection Security Agreement (ISA).
    - Computer Matching Agreement (CMA).
    - Information Exchange Agreement (IEA).
- CMS Minimum Acceptable Risk Standards for Exchanges (MARS-E) Document Suite.
- National Institutes of Standards and Technology (NIST) Special Publications (SP) such as:
    - SP 800-88 Revision 1 (draft), Guidelines for Media Sanitization, September 2012.
    - SP 800-147, BIOS Protection Guidelines, April 2011.
    - SP 800-160 Initial Public Draft System Security Engineering An Integrated Approach to Building Trustworthy Resilient Systems (Section 3.11)

Office of Management and Budget (OMB) Circular NO. A-130, Revised, Management of Federal Information Resources, Nov 2000.

The primary system transition, decommission and data mitigation activities are described in greater detail in the remainder of this document. This document primarily describes activities that will require considerable involvement by states, including the submission of action plans, activities, and other relevant information to CMS. If any step is not applicable or cannot be completed, the rationale must still be documented and submitted to CMS for review. CMS will evaluate the information submitted by states, approve or disapprove, and require updates accordingly before execution of planned activities are allowed to be conducted.

MARKETPLACE IT SYSTEMS AND DATA MIGRATION ACTIVITIES

Table 1: IT Systems and Data Migration Activities

Task	Task Name	Description
1	Overall Migration Plan	• Describe the business functions from the Marketplace IT system that will be supported by the FFM. Discuss the type of data (e.g., information classes/data subject areas) maintained in the Marketplace IT system that will be migrated to be included in the FFM. • Describe the Marketplace IT system structure and major components and designate which system components will and will not be migrated. If the migration process will be organized into discrete phases, identify which system components will undergo migration in each phase. Address in explicit subsections the migration overview associated with hardware, software, and data, as appropriate. • Work with CMS to define the data migration strategy, data quality assurance, and data migration controls. Describe how data will be migrated, measured, and secured; the controls that will be in place to ensure that data migration has been successful; and any requirements associated with maintaining/transferring authoritative data source (ADS) designations or related service-level agreements (SLA). Describe the major risk factors in the data migration effort and strategies for their control or reduction. • Describe efforts to maintain the confidentiality, integrity, and availability of sensitive data (i.e., personally identifiable information or tax information) currently hosted in the system to be

		decommissioned until it is verified as destroyed and not retrievable.
1.1	Hardware and Software Migration	Work with CMS to define an overall strategy and activities required needed for the migration from Marketplace IT system hardware and software to the FFM. List and describe the Marketplace hardware and software that will continue to be used and will no longer be used.
1.2	Data Migration Requirements	Work with CMS to define the specific data preparation requirements and the Marketplace data that must be available for the migration. If data will be transported from the original Marketplace IT system, work with CMS to define a detailed description of data handling, migration, and loading procedures. If the data will be transported using machine-readable media, describe the characteristics of each media component.
1.3	Data Migration Mapping	List and account for all data mapped to the Marketplace IT system in terms of where and when it will be migrated.
1.4	Data Migration Security Requirements	• Work with CMS to define security requirements for establishing connections between the state Marketplace IT system and the FFM when migrating data. • Work with CMS to outline data security and associated risk mitigation strategies. Identify the impacts to Marketplace IT and/or the FFM during the data migration and develop a strategy for mitigating the risks. Specifically, identify what security controls will be implemented during the migration process, for example: o Access controls: Access to/responsibility for the data during the entire process is documented. o Configuration management: Validated effective and operational functions maintain data integrity. o Change management: Documented process for requesting, approving, and implementing changes to IT systems and supporting operational processes as it specifically applies to the FFM data migration. o Contingency planning: An exact copy of data is maintained during the migration process in case of a failure. o Identification and authentication: All hardware is authenticated before the migration process is initiated. Encryption is implemented for data transmission. o Planning: System Security Plan is updated as components of the Marketplace IT system are decommissioned. o Risk management: Mitigation plans are documented and implemented to address known and potential risks/vulnerabilities during the migration process. o Media sanitization: Hardware is tested to ensure data is destroyed and not retrievable. o Privacy impact assessment (PIA): The PIA is updated and validated.
1.5	Legal Agreements	Coordinate with CMS to establish a memorandum of understanding (MOU), or similar legal agreement, to document data migration security requirements.
1.6	Impact to Other	Describe the state Marketplace IT system's interfaces to other state,

	System Interfaces	issuer, Federal, and agency systems that will be affected by the data migration. List each affected interface and the necessary changes to support or eliminate the interface upon migration.
1.7	Test Plan	Work with CMS to define the testing that will be conducted to ensure that all migration activities are successful. At a minimum, include who will perform the testing, the test cases that will be performed, and how the results of the testing will be tracked and reported.
1.8	Migration Schedule	Create a work breakdown schedule (WBS) consisting of activities, tasks, milestones, and a fully developed test plan. Identify critical design reviews, indicating progress of the migration itself.
1.9	Migration Resources	Describe the state resources necessary to perform the migration. Highlight required hardware, software, people, and facility resources not currently available and detail an approach for obtaining all currently unavailable resources.
1.10	Administrative Responsibilities	• Describe the process and the steps taken to ensure all old legal contracts and agreements (including service-level agreements) have been closed and nullified. • Describe the process and the steps taken to implement new agreements, as required, including roles and responsibilities for signatures and approvals.

Perform Migration Activities

All documentation included in Table 1 must be submitted to CMS for approval before any migration activities can occur. The migration should be performed based on the approved migration plan in Table 1. This step should not be initiated until the necessary migration resources outlined in the plan are available and risks have been accepted or mitigated. At the end of the migration, the state project manager will coordinate management approvals of documentation created during the activity. Management approval and acknowledgement will be formally documented and the final documentation must be submitted to CMS.

MARKETPLACE IT SYSTEMS AND DATA DECOMMISSION ACTIVITIES

All activities involved in the establishment and execution of the state Marketplace IT system decommission are listed below. The first decommissioning activity is the development of a decommission plan for the Marketplace IT system. Upload all decommissioning artifacts into CALT.

Table 2: IT Systems and Data Decommission Activities

Task	Task Name	Description
2	Marketplace IT Decommission Plan	Work with CMS to develop the decommission plan. The decommission plan ensures the decommissioning of the Marketplace IT system is planned and executed in a way that data and application logic are preserved, affected parties are appropriately notified, and disposition of hardware and software is conducted in compliance with established state and Federal guidelines. The remaining tasks within this table describe the various tasks required for the system decommission.

2.1	Software Archival	Describe the activities for archiving the software library files and related documentation in the system being decommissioned, including which software will be archived, and in which format. The intent of the software archive is to provide sufficient stored software so the system could be re-initiated if necessary.
2.2	Documentation Archival	Describe the activities for archiving the hard copy and soft copy user documentation for the Marketplace IT, including which documentation will be archived and in which format. The intent of the documentation storage is to provide sufficient archived documentation so the system could be re-initiated and used if necessary.
2.3	Hardware Disposition	Describe the activities for disposing of hardware that was used exclusively by the state Marketplace IT system, including the methodology for ensuring data cannot be retrieved from the decommissioned equipment.
2.4	Data Retention and Destruction	Describe the activities for retaining data files and related documentation of the system being decommissioned and the length of that retention period. Outline which data have been migrated, which data will be retained, and in which format, and which data will be destroyed. 45 CFR §155.1210 Maintenance of Records, states the SBMs must maintain and ensure its contractors, subcontractors, and agents maintain certain documents and records for ten years. These documents and records (whether paper, electronic, or other media) and other evidence of accounting procedures and practices, must be sufficient to: accommodate periodic auditing of financial records, and enable the US Department of Health and Human Services (HHS) or its designee(s) to inspect facilities, or otherwise evaluate the SBM's compliance with Federal standards.
2.5	Legal Agreements, System Security Plan, and Associated Artifacts	• Coordinate with CMS to update legal agreements established between CMS and the state to allow connection to the FDSH. States may need to change the state signatory on the legal agreements. • Update and retain the system security plan (SSP), which should describe the system security and access rights associated with the Marketplace IT system. The SSP should describe the necessary security information so the system could be reconstituted with the same security considerations, if necessary. • Update the IRS Safeguard Security Report and submit to IRS at safeguardreports@irs.gov. This report is the primary source for the state to report to IRS on the processes, procedures, and security controls in place to protect Federal Tax Information (FTI) and must be submitted annually in accordance with IRC 6103(p)(4), as long as FTI is retained. Additionally, the state may not transfer the custody of FTI to another state agency (or vendor) before notification and approval of the IRS.
2.6	Decommission Schedule	Provide a WBS that consists of the activities, tasks, milestones, and review points for the decommission itself.
2.7	Decommission Resources	Describe the state resources necessary to perform the decommission activities, including identification of required hardware, software, people, and facility resources and a detailed approach for obtaining all currently

		unavailable resources.

Perform Decommission Activities

All documentation included in Table 2 must be submitted to CMS for approval before any decommission activities can occur. The system decommission should be performed based on the approved decommission plan. This step should not be initiated until the necessary decommissioning resources outlined in the plan are available and risks have been accepted, eliminated, or mitigated. At the end of the decommission process, the state project manager will coordinate management approvals of documentation created during the activity. Management approval and acknowledgement must be formally documented and the final documentation must be submitted to CMS.

Appendix F:

Federal Exchange Fee Range

Net Premium and Estimated Federal Fee by Family Size and Income

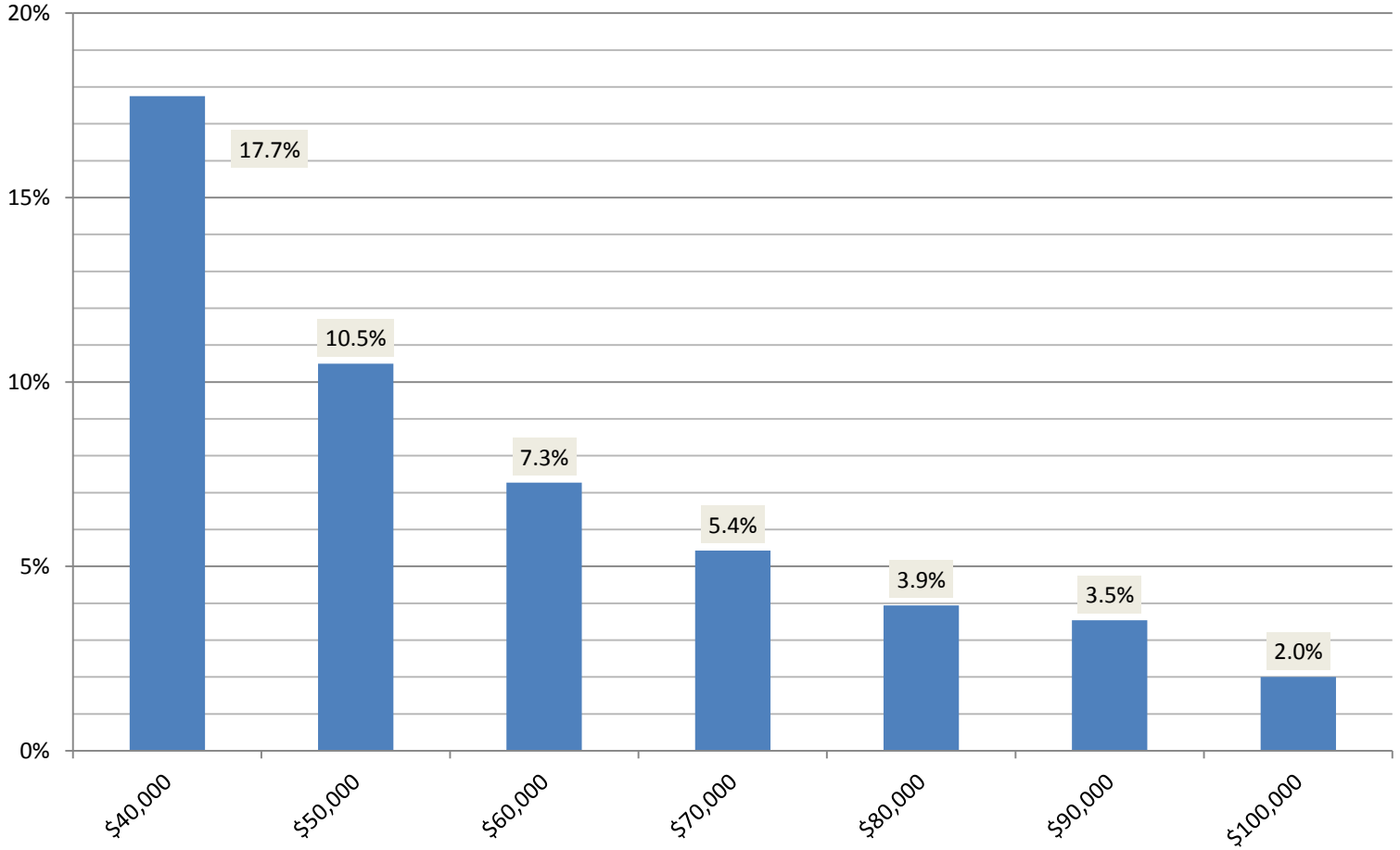
Net Premium and Estimated Federal Fee for Most Popular Health Plan				
4-Person Household (assumes 2 dependents in college) *Based on 2016 premium and subsidies for BCBSVT Standard Silver Family Plan*				
Assuming Federal Exchange Fee of:		2.0%	2.8%	3.5%
Monthly Fee Would be:		$27	$38	$48
Annual Income	Net Premium after APTC & VPA	Fee as % of Net Premium	Fee as % of Net Premium	Fee as % of Net Premium
$20,000	N/A (Medicaid)	0%	0%	0%
$30,000	N/A (Medicaid)	0%	0%	0%
$40,000	$153	17.7%	24.8%	31.1%
$50,000	$259	10.5%	14.7%	18.4%
$60,000	$374	7.3%	10.2%	12.7%
$70,000	$501	5.4%	7.6%	9.5%
$80,000	$690	3.9%	5.5%	6.9%
$90,000	$770	3.5%	4.9%	6.2%
$100,000	$1,361	2.0%	2.8%	3.5%
$110,000	$1,361	2.0%	2.8%	3.5%

Net Premium and Estimated Federal Fee for Most Popular Health Plan				
2-Person Household *Based on 2016 premium and subsidies for BCBSVT Standard Silver Couple Plan*				
Assuming Federal Exchange Fee of:		2.0%	2.8%	3.5%
Monthly Fee Would be:		$19	$27	$34
Annual Income	Net Premium after APTC & VPA	Fee as % of Net Premium	Fee as % of Net Premium	Fee as % of Net Premium
$20,000	N/A (Medicaid)	0%	0%	0%
$30,000	$142	13.6%	19.1%	23.9%
$40,000	$257	7.5%	10.6%	13.2%
$50,000	$435	4.5%	6.2%	7.8%
$60,000	$516	3.8%	5.3%	6.6%
$70,000	$969	2.0%	2.8%	3.5%
$80,000	$969	2.0%	2.8%	3.5%
$90,000	$969	2.0%	2.8%	3.5%
$100,000	$969	2.0%	2.8%	3.5%
$110,000	$969	2.0%	2.8%	3.5%

Net Premium and Estimated Federal Fee for Most Popular Health Plan				
1-Person Household *Based on 2016 premium and subsidies for BCBSVT Standard Silver Single Plan*				
Assuming Federal Exchange Fee of:		2.0%	2.8%	3.5%
Monthly Fee Would be:		$10	$14	$17
Annual Income	Net Premium after APTC & VPA	Fee as % of Net Premium	Fee as % of Net Premium	Fee as % of Net Premium
$20,000	$74	13.0%	18.2%	22.8%
$30,000	$186	5.2%	7.3%	9.1%
$40,000	$338	2.9%	4.0%	5.0%
$50,000	$484	2.0%	2.8%	3.5%
$60,000	$484	2.0%	2.8%	3.5%
$70,000	$484	2.0%	2.8%	3.5%
$80,000	$484	2.0%	2.8%	3.5%
$90,000	$484	2.0%	2.8%	3.5%
$100,000	$484	2.0%	2.8%	3.5%
$110,000	$484	2.0%	2.8%	3.5%

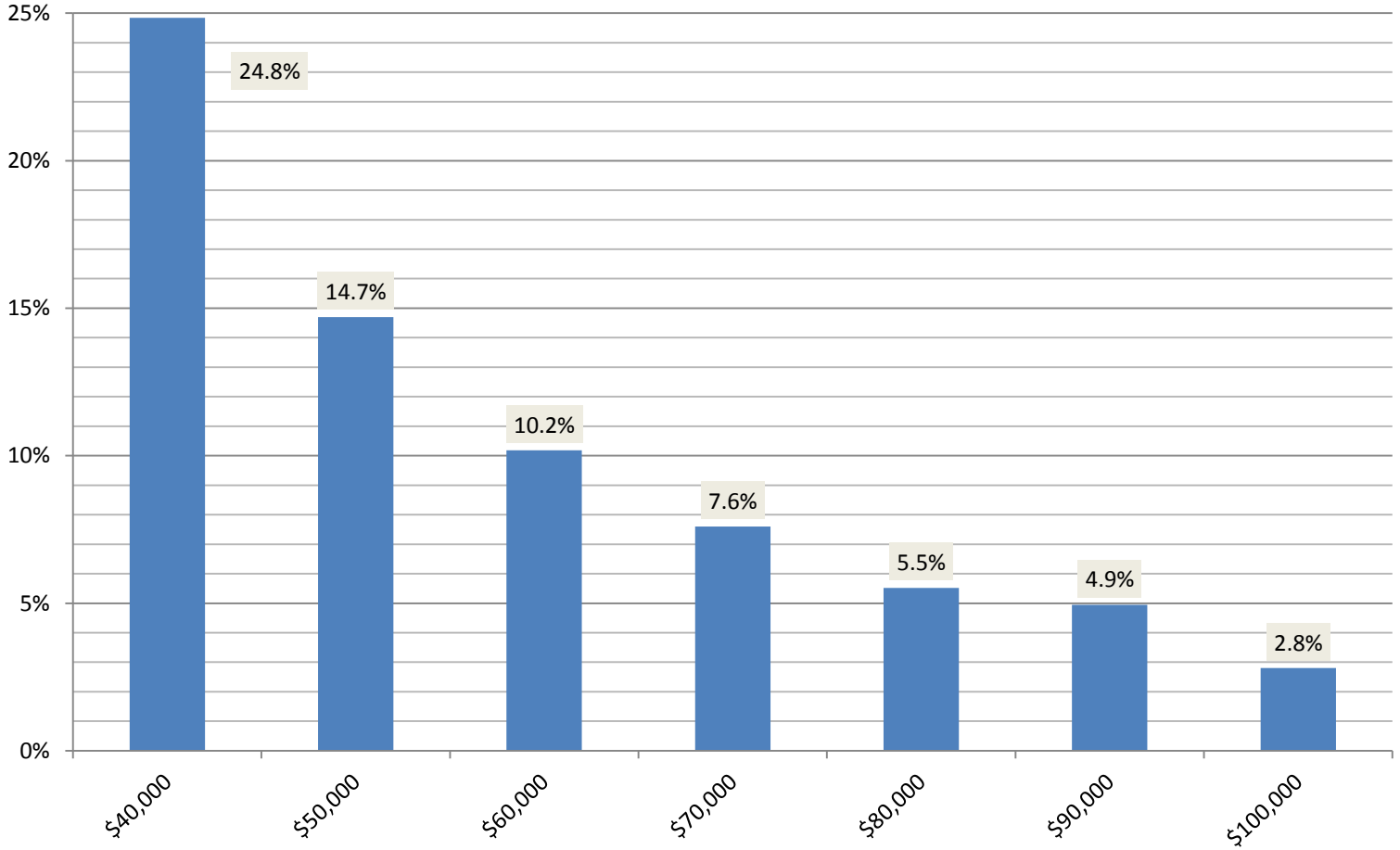
Federal Exchange Fee Paid by Household Income

(2.0% Fee as % of Family of Four's Net 2016 Premium)



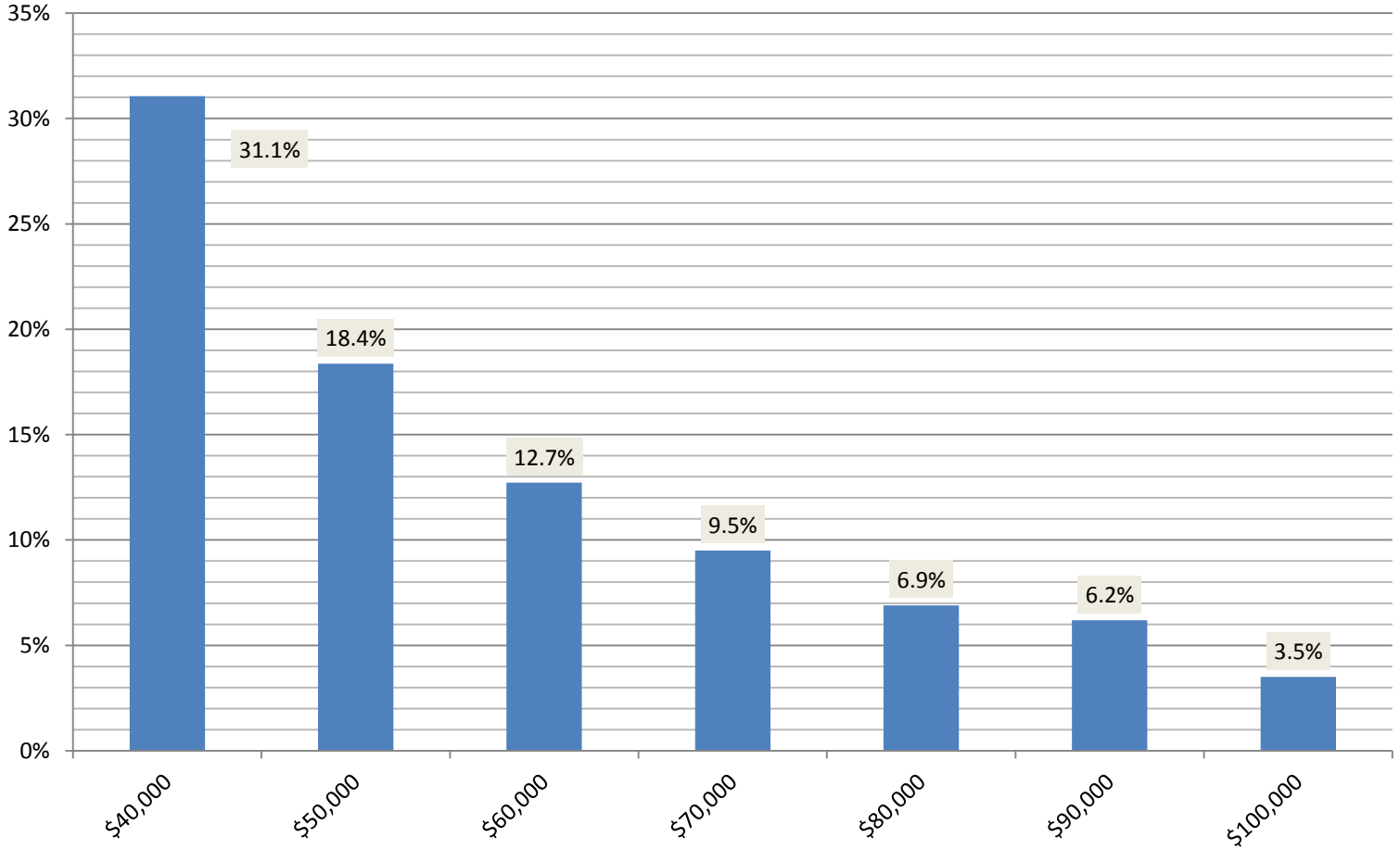
Federal Exchange Fee Paid by Household Income

(2.8% Fee as % of Family of Four's Net 2016 Premium)



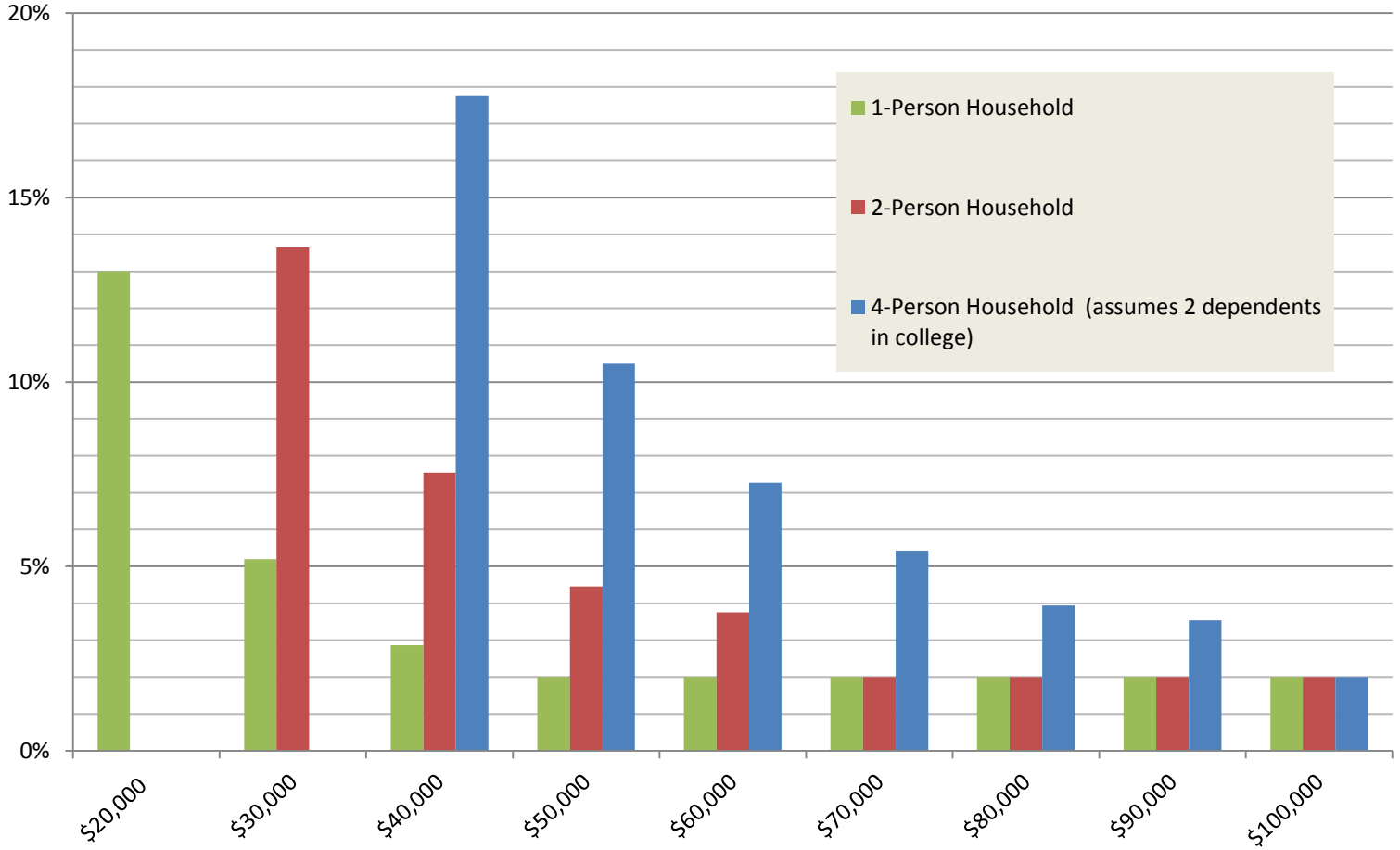
Federal Exchange Fee Paid by Household Income

(3.5% Fee as % of Family of Four's Net 2016 Premium)



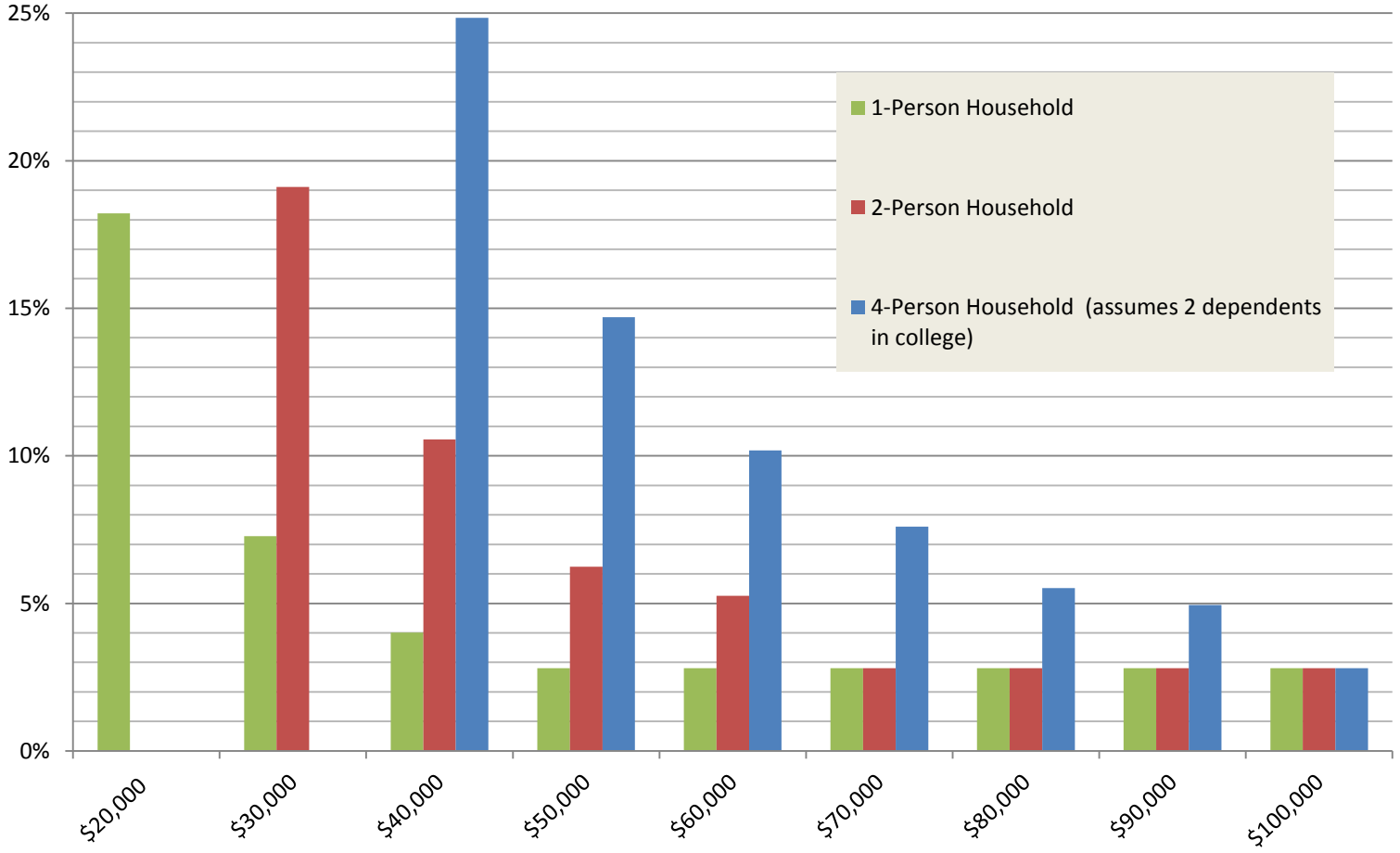
Federal Exchange Fee Paid by Household Income

(2.0% Fee as % of Household's Net 2016 Premium)



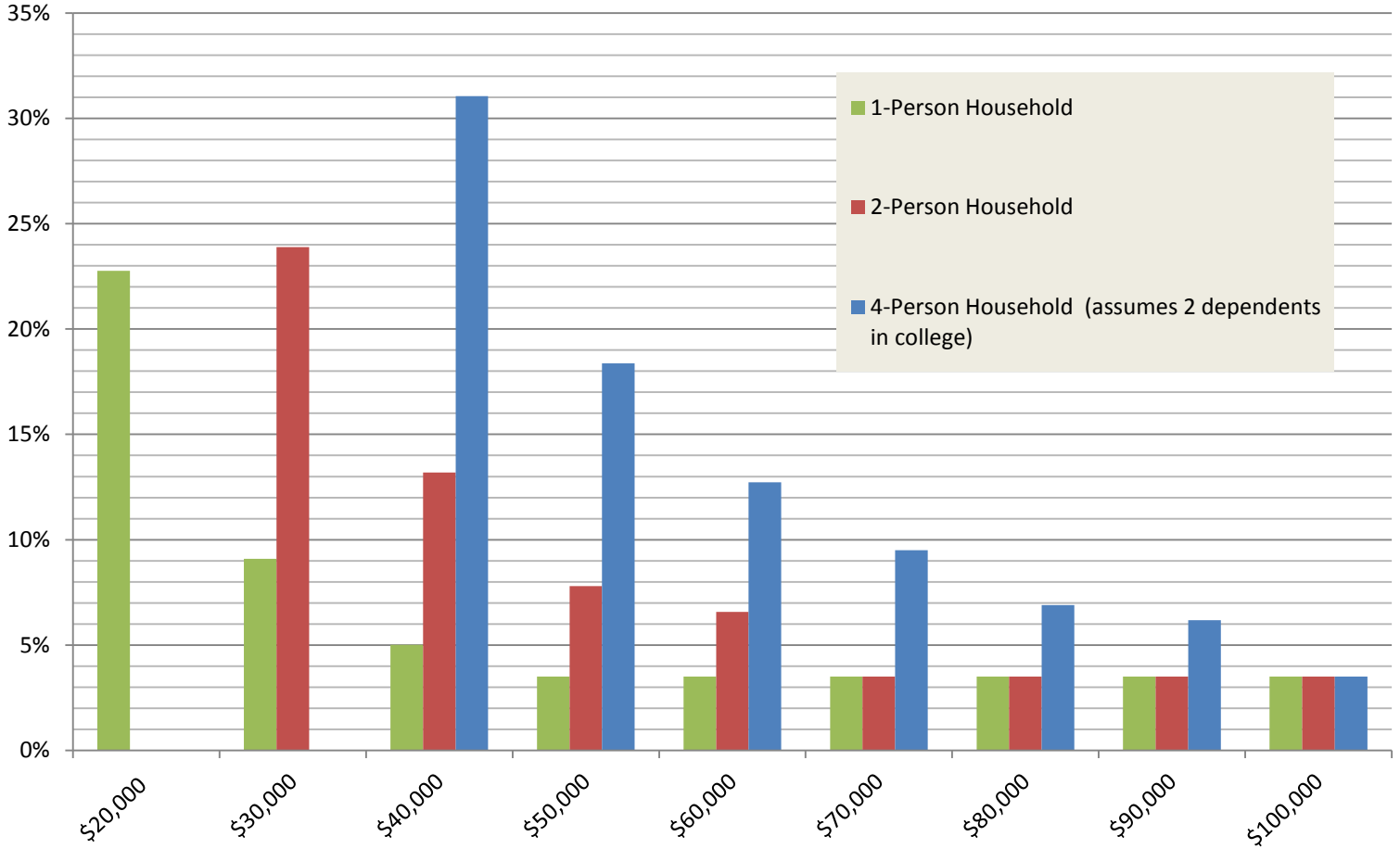
Federal Exchange Fee Paid by Household Income

(2.8% Fee as % of Household's Net 2016 Premium)



Federal Exchange Fee Paid by Household Income

(3.5% Fee as % of Household's Net 2016 Premium)



Appendix. F. Net Premium and Estimated Federal Fee by Family Size and Income

1-Person Household *Based on 2016 premium and subsidies for BCBSVT Standard Silver Single Plan*				
Assuming Federal Fee of:		2.0%	2.8%	3.5%
Monthly Fee Would be:		$10	$14	$17
Annual Income	Net Premium after APTC & VPA	Fee as % of Net Premium	Fee as % of Net Premium	Fee as % of Net Premium
$20,000	$74	13.0%	18.2%	22.8%
$30,000	$186	5.2%	7.3%	9.1%
$40,000	$338	2.9%	4.0%	5.0%
$50,000	$484	2.0%	2.8%	3.5%
$60,000	$484	2.0%	2.8%	3.5%

2-Person Household *Based on 2016 premium and subsidies for BCBSVT Standard Silver Couple Plan*				
Assuming Federal Fee of:		2.0%	2.8%	3.5%
Monthly Fee Would be:		$19	$27	$34
Annual Income	Net Premium after APTC & VPA	Fee as % of Net Premium	Fee as % of Net Premium	Fee as % of Net Premium
$20,000	N/A (Medicaid)	0%	0%	0%
$30,000	$142	13.6%	19.1%	23.9%
$40,000	$257	7.5%	10.6%	13.2%
$50,000	$435	4.5%	6.2%	7.8%
$60,000	$516	3.8%	5.3%	6.6%
$70,000	$969	2.0%	2.8%	3.5%
$80,000	$969	2.0%	2.8%	3.5%

4-Person Household (assumes 2 dependents in college) *Based on 2016 premium and subsidies for BCBSVT Standard Silver Family Plan*				
Assuming Federal Fee of:		2.0%	2.8%	3.5%
Monthly Fee Would be:		$27	$38	$48
Annual Income	Net Premium after APTC & VPA	Fee as % of Net Premium	Fee as % of Net Premium	Fee as % of Net Premium
$20,000	N/A (Medicaid)	0%	0%	0%
$30,000	N/A (Medicaid)	0%	0%	0%
$40,000	$153	17.7%	24.8%	31.1%
$50,000	$259	10.5%	14.7%	18.4%
$60,000	$374	7.3%	10.2%	12.7%
$70,000	$501	5.4%	7.6%	9.5%
$80,000	$690	3.9%	5.5%	6.9%
$90,000	$770	3.5%	4.9%	6.2%
$100,000	$1,361	2.0%	2.8%	3.5%