COPY – I.D

Contract #

4000013930

PENNSYLVANIA DEPARTMENT OF HUMAN SERVICES

Bureau of Procurement and Contract Management

CONTRACT AMENDMENT

Medicaid Management Information System Agreement Amendment # 7

Gainwell Technologies, LLC
355 Ledgelawn Drive
Conway, AR 72034-9501
scott.philp@gainwelltechnologies.com
Federal I.D. Number: 27-1510177
SAP Vendor Number: 542948

Office of Medical Assistance Programs
Sandy Marcella
samarcella@pa.gov
(717) 772-6276

For Program Office/Facility Use Only

Are multiple agreements of this type expected? Yes ☐ No ☒

If yes, avoid multiple rejections by submitting one agreement and using BPCM's feedback to improve the remaining agreements.

AMENDMENT NUMBER SEVEN TO
CONTRACT NO. 4000013930

This Amendment Number Seven (“Amendment No. 7”) is made and entered into by and between the Commonwealth of Pennsylvania through the Department of Human Services, formerly Department of Public Welfare, (“Department” or “DHS”) and Gainwell Technologies, LLC (formerly, Enterprise Services LLC, a wholly owned subsidiary of DXC Technology Company, formerly, HP Enterprise Services LLC., and formerly Electronic Data System (“Contractor”)).

WITNESSETH:

WHEREAS, on the 1st of November 2009, the DHS and Contractor entered into a contract regarding the transition, modification, operation and maintenance and turnover of the Medicaid Management Information System (known as “PROMIS*e*™”), which provides automated support for the Medical Assistance Program as well as other Commonwealth programs (the “Contract”);

WHEREAS, throughout the Contract term, DHS and Contractor have agreed to six Contract Amendments;

WHEREAS, Department wishes to add an additional performance standard regarding the National Correct Coding Initiative (“NCCI”);

WHEREAS, the Department has identified a need to expand Electronic Visit Verification services to include Home Health Services;

WHEREAS, the Department has identified a need to expand the Fraud, Waste and Abuse services to include case tracking and to upgrade the existing technology;

WHEREAS, the Department has identified a need to increase the estimated maximum number of hours for payment for Modifications to support Medicaid Management Information System (“MMIS”) Modernization;

WHEREAS, the Department has identified a need to include the term Transformed – Medicaid Statistical Information System as part of the contract requirements related to Management and Administrative Reporting (“MAR”) and Medicaid Statistical Information System (“MSIS”):

WHEREAS, Contractor now wishes to migrate the legacy PROMIS*e*™ platform from a the Contractor hosted data center to the Amazon Web Services (“AWS”) Cloud Computing Services;

WHEREAS, the Department has received conditional approval from the Governor’s Office of Administration for the move to the cloud environment; and

WHEREAS, in accordance with Section 5 of the Contract, the parties are amending certain portions of the Contract as set forth in this Amendment No. 7.

NOW, THEREFORE, the Parties, intending to be legally bound, agree:

1. Section 3 of the Contract of MMIS Contractor services is amended by the addition of the attached Appendices as Appendix F Requirements for Non-Commonwealth Hosted Applications/Services, Appendix G Framework for Independent Third-Party Security and Privacy Assessment Guidelines for Medicaid Enterprise Systems ("MES"), and Appendix H FraudCapture™ Services Supplement, as follows:

3. The services described in section 2 above shall be provided in conformity with this Contract, as amended, and the following:

Appendix A Pennsylvania MMIS Terms and Conditions, as amended

Appendix B-2 Payment Provisions

Appendix C Work Statement

Appendix D RFP No. 41-08, excluding Appendices A-D, F, G, I-K, M, P-Q, and S-U, as amended and including MMIS RFP 41-08 Amendments and Questions and Answers dated October 31, 2008.

Appendix E Contractor's Proposal, consisting of:

- Contractor's Technical Submittal dated January 20, 2009, including Contractor's Oral Presentation and Responses dated February 24, 2009
- Contractor's Final Disadvantaged Business Proposal dated January 20, 2009, as amended by letter dated August 7, 2009
- Contractor's Domestic Workforce Utilization Submittal dated January 20, 2009
- Contractor's Contractor Partnership Submittal dated January 20, 2009

Appendix F Requirements for Non-Commonwealth Hosted Applications/Services

Appendix G Framework for Independent Third-Party Security and Privacy Assessment Guidelines for Medicaid Enterprise Systems (MES) (the "CMS Framework")

- Annually, to coincide with each State Fiscal Year ("SFY"), the Contractor will arrange for third-party audits to satisfy both the SOC 2 Type II and CMS Framework requirements.
  - For SFY 2021-2022, Contractor will arrange for the following audit activities:
    - SOC2 Type 2 Readiness Assessment
  - For SFY 2022-2023, Contractor will arrange for the following audits or audit activities:
    - SOC2 Type 2 Audit (7/1/22 – 9/30/22 assessment period – delivered December 2022)
    - SOC2 Type 2 Audit (10/1/22 – 6/30/23 assessment period – delivered September 2023)

    - Independent Third-Party Security and Privacy Assessment (delivered July 2023). This assessment will address items in the CMS Framework not addressed by the SOC2 Type 2 audit.
  - The month following the completion of the Readiness Assessment or the delivery of an audit report, Contractor will invoice the Department for 75% of actual 3rd party costs it incurred with respect to conducting the audit or audit activity.
  - The Contractor shall timely remediate any application and/or system security, data security, and privacy vulnerabilities exposed through these audits and assessments.

Appendix H FraudCapture™ Services Supplement

The above Appendices are incorporated by reference and made part of the Contract.

2. **Appendix A Pennsylvania MMIS Terms and Conditions.** Appendix A Pennsylvania MMIS Terms and Conditions is amended as follows:

a. The following is added to Section 8.1 Consequential Damages as *Subsection A-8.1.4 Transformed Medicaid Statistical Information System ("T-MSIS") Reporting*:

A-8.1.4 Transformed Medicaid Statistical Information System ("T-MSIS") Reporting

A-8.1.4.1 T-MSIS Reporting – Performance Requirements

Contractor shall submit T-MSIS files to CMS according to the published CMS schedule and will ensure files are created according to Department approved crosswalks. Contractor shall monitor the CMS website on a weekly basis for Pennsylvania's T-MSIS status and work collaboratively with the Department to resolve T-MSIS Priority Issues ("TPIs") and Data Quality ("DQ") issues within the Contractor's control.

A-8.1.4.2 T-MSIS Reporting –Damages

Contractor shall be liable for the difference between the maximum allowable enhanced federal financial participation ("FFP") and the FFP actually received by the Department as a result of the failure of the Contractor to comply with the T-MSIS requirements. Contractor shall be accountable only for those damages that arise from its own acts or omissions.

While the Contractor will work with the Department to resolve all data quality issues within the Contractor's domain, the Contractor shall not be held non-compliant for data quality issues caused by items outside of the Contractor's control such as documented Client Information System (CIS) defects, inaccurate program data, or invalid/inaccurate data received from Providers/MCOs.

The Department shall notify the Contractor within three (3) days of receiving notification from CMS of non-compliance causing FFP to be withheld.

Should the Contractor not be solely responsible for the Department losing FFP, damages will be allocated to reflect only the portion which is the Contractor's responsibility. The Department will withhold from monies payable to Contractor all FFP penalty claims assessed by CMS until all such damages are satisfied.

b. The following is added to Section A-8.2 Liquidated Damages as *Subsection A-8.2.16 Compliance with Medicaid National Correct Coding Initiative Technical Guidance Manual*:

A-8.2.16 Compliance with Medicaid National Correct Coding Initiative Technical Guidance Manual

A-8.2.16.1 Compliance with Medicaid National Correct Coding Initiative Technical Guidance Manual - Performance Requirements

Contractor must implement quarterly Medical Assistance ("MA") NCCI edits (new, revised and deleted) at the direction of the Department. Contractor shall not disclose any of these edits prior to the start of a new calendar quarter other than through a disclosure of non-confidential information available to the general public and published on the Medicaid NCCI webpage. Contractor shall not publish or share edits with individuals, medical societies or any other entities prior to publication on the Medicaid NCCI webpage and only after Department approval.

Contractor shall not enable NCCI edits within PROMIS*e*™ prior to the effective date of the edit.
Contractor shall only use non-public information from the quarterly Medicaid NCCI edit file for business purposes directly related to the implementation of the Medicaid NCCI methodologies as directed by the Department.

A-8.2.16.2 Compliance with Medicaid National Correct Coding Initiative Technical Guidance Manual - Liquidated Damages

The Department may assess liquidated damages in an amount up to $500.00 for each incidence of non-compliance with the NCCI performance requirement. Performance requirement is defined as 1) Sharing the NCCI data with an outside entity or 2) Publishing the data early within MMIS. Liquidated damages assessed with respect to the NCCI performance requirement shall not exceed $5,000 per month.

3. **Appendix A – Pennsylvania MMIS Terms and Conditions.** Appendix A Pennsylvania MMIS Terms and Conditions Subsection A-8.11 is amended by the addition of the following as the last paragraph to Subsection A-8.11:

Upon the full execution of this Amendment No. 7, the Commonwealth approves Contractor's use of AWS as a subcontractor as provided in this Amendment No. 7. Contractor shall use Health Insurance Portability and Accountability Act compliant AWS cloud services offering under its global procurement agreement with AWS. Contractor's use of AWS shall conform to all representations made in Contractor's Cloud Use Case presented to the Commonwealth. If Contractor plans to modify any aspect of cloud use set up and security, it shall notify the Department and shall obtain Cloud Use Case approval prior to implementing the modification.

4. **Appendix A – Pennsylvania MMIS Terms and Conditions**. Appendix A Pennsylvania MMIS Terms and Conditions is amended by deleting Appendix A-4-2 List of Contractor Software and replacing it with the attached Appendix A-4-3 List of Contractor Software, and by deleting Appendix A-5-2 List of Third-Party Software and Tools in Use and replacing it with the attached Appendix A-5-3 List of Third-Party Software and Tools in Use.

5. **Appendix B-2 Payment Provisions – Section 6.** Section 6 Payment for Operation and Maintenance of Appendix B-2 Payment Provisions, as amended in Amendment No. 6, is further amended as follows:

a. Subsection 6 EVV immediately preceding the section titled ePrescribing Operations and Maintenance Fee is deleted and replaced with the following:

EVV Services: The Department will pay a monthly all-inclusive fee for the maintenance and support of the EVV as follows:

Personal Care EVV Services	$245,285.50

Following the Department sign-off of the testing results and the production approval documents according to the Change Control Process, the Home Health EVV functionality and services will Go Live on the agreed upon date. Beginning with the first full calendar month following the Go Live date, the Department will pay the following monthly all-inclusive fee for the maintenance and operations of the Home Health EVV Services. Should system issues require the EVV Home Health functionality to be backed-out of Production or turned off in Production, the Department will cease Home Health EVV monthly payments until the system is redeployed or turned on following the Change Control Process. Should post-release issues occur which don't require the EVV Home Health functionality to be backed-out or turned off, the normal Change Order and/or Defect processes will be followed to correct the issues and the monthly fee will continue.

Home Health EVV Services	$235,443.00

b. The following paragraphs are added immediately following the ePrescribing Operations and Maintenance Fee section:

Fraud, Waste and Abuse Services:

Following the Department sign-off of the testing results and the production approval documents according to the Change Control Process, the FraudCapture functionality and services will Go Live on the agreed upon date. Beginning with the first full calendar month following the Go Live date, the Department will pay the following monthly all-inclusive fee for the maintenance and operations of the FraudCapture Services. Should system issues require the FraudCapture functionality to be backed-out of Production or turned off in Production, the Department will cease FraudCapture monthly payments until the system is redeployed or turned on following the Change Control Process. Should post-release issues occur which don't require the FraudCapture functionality to be backed-out or turned off, the normal Change Order and/or Defect processes will be followed to correct the issues and the monthly fee will continue.

Operations Phase – 8/1/2022 (anticipated implementation) - 10/31/2022: $179,388
Operations Phase (Option Year 2) – 11/1/2022 – 10/31/2023: $180,882

Contractor shall comply with all FraudCapture Performance Standards and Contractor Responsibilities set forth in the FraudCapture Statement of Work.

Beginning with the month in which the Department begins making the payments described above with respect to FraudCapture, Contractor shall reduce its semi-monthly fee listed in the Pricing Table for Operations including Maintenance as follows:

Contract Period	Contract Year	Semi-Monthly Fixed Fee
16	11/01/2021-10/31/2022	$1,200,309.12
17	11/01/2022-10/31/2023	$1,200,309.12

c. The Section 6 paragraph and table of monthly reductions to Operations fee that immediately precedes the section titled Pricing Table for Optional Provider Service Center is deleted and replaced with the following:

If PROMIS*e*™ functionalities or services are replaced or transitioned to another contract, Contractor shall reduce the semi-monthly or monthly fees for operations and maintenance beginning in the first full month following the successful transition of the functionality or service. For those functionalities or services that are paid based on a monthly fee for their operation and maintenance, Contractor shall reduce its fee by the amount of that monthly fee. Currently, these functionalities and services include the User Acceptance Test Environment, K2 Blackpearl Software, EVV (Home Health and Personal Care), ePrescribing, and LIHEAP, and will include

Fraud, Waste and Abuse. For those functionalities or services that are paid on a semi-monthly basis, Contractor and the Department will negotiate a reduction in that semi-monthly fee in accordance with Appendix A, Section A-2.5.

Appendix H has been added as a services supplement for the FraudCapture product.

6. **Appendix B-2 Payment Provisions**. Section 7 Payment for Modifications of Appendix B-2 Payment Provisions, as amended in Amendment No. 6, is amended to delete the first paragraph and accompanying table and to replace it with the following:

The Contractor will be reimbursed for actual hours expended during a month working on DHS approved change orders at the blended rate per hour for the applicable period of the Contract. For each approved change order, the total number of hours billed by the Contractor may not exceed the approved budget for the change order per the change control process, which may be changed from time to time. The all-inclusive blended hourly rate for each contract year is as follows:

Contract Period	Contract Year All Inclusive Hourly	Blended Rate	Estimated Number of Hours	Annual Amount
l	11/01/09 - 6/30/2010	$91.03	20,000	$1,820,600
2	SFY 10-11	$93.08	30,000	$2,792,400
3	SFY 11-12	$95.17	30,000	$2,855,100
4	SFY 12-13	$97.31	30,000	$2,919,300
5	SFY 13-14	$99.50	30,000	$2,985,000
6	SFY 14-15	$101.74	30,000	$3,052,200
7	7/01/15 - 10/31/2015	$104.03	10,000	$1,040,300
8	11/1/15-6/30/16	$106.37	20,000	$2,127,400
9	SFY16-17	$106.37	30,000	$3,191,100
10	7/01/17 - 10/31/2017	$106.37	10,000	$1,063,700
11	11/01/17 - 6/30/2018	$106.37	20,000	$2,127,400
12	SFY 18 -19	$106.37	30,000	$3,191,100
13	SFY 19 -20	$106.37	30,000	$3,191,100
14	7/01/20 - 10/31/2020	$106.37	10,000	$1,063,700
15	11/01/2020 - 6/30/2021	$110.47	20,000	$2,209,400
16	7/01/2021 - 10/31/2021	$110.47	10,000	$1,104,700

17	11/01/2021 - 6/30/2022	$112.46	35,000	$3,936,100
18 (Option Year)	7/01/2022 - 10/31/2022	$112.46	20,000	$2,249,200
19 (Option Year)	11/01/2022 - 6/30/2023	$114.06	35,000	$3,992,100
20 (Option Year)	7/01/2023 - 10/31/2023	$114.06	25,000	$2,851,500

7. **TERM OF AMENDMENT:** The Effective Date of this Amendment will be the date that this amendment is fully executed by DHS and Contractor and all approvals required by the Commonwealth and federal contracting procedures have been obtained. This Amendment shall continue in effect coterminous with the term of the Contract, as amended.

8. **DEFINITIONS:** Except as defined herein, or otherwise required by the context herein, all defined terms used in this Amendment shall have the meanings set forth in the Contract, as amended.

9. **CONTRACT TERMS:** Except as explicitly provided for in this Amendment No. 7, all other provisions of this Contract and Amendments 1 through 6, shall remain unchanged and in full force and effect.

[Remainder of page intentionally left blank.]

IN WITNESS WHEREOF, the Parties, through their authorized representatives, have properly executed this Amendment No. 7 to the Contract on the date of the last Commonwealth signature below.

COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF HUMAN SERVICES

Ally Wullbrandt Digitally signed by Ally Wullbrandt
Date: 2022.04.04 15:02:07 -04'00'

SECRETARY/designee Date

GAINWELL TECHNOLOGIES LLC

DocuSigned by:
Paul Saleh
C5B903FEA402401... 3/22/22

Date

Paul Saleh President and CEO

Printed Name and Title

Ann Lefevre Digitally signed by Ann Lefevre
Date: 2022.05.13 11:06:06 -04'00'

COMPTROLLER Date

APPROVED AS TO FORM AND LEGALITY

Digitally signed by Lara Antonuk
Date: 2022.04.15 16:07:51 -04'00'

OFFICE OF GENERAL COUNSEL Date
DEPARTMENT OF HUMAN SERVICES

Pamela J. Cross 2022.04.20 10:02:58 -04'00'

OFFICE OF GENERAL COUNSEL Date

Digitally signed by David E. Stover, Senior Deputy Attorney General
Date: 2022.05.04 14:51:30 -04'00'

OFFICE OF ATTORNEY GENERAL Date

APPENDIX A-4-3

In accordance with section A-5.2.2.3, Expiration or Termination Non-exclusive License Grant- Tools and Software of Appendix A, Contractor will provide the listed software and tools to the Department at the end of the Contract unless otherwise noted below.

Software/Tools Name	Function	Notation
Project Workbook	Document repository for system documentation, change orders, and project related information	
DSS Profiler	Fraud and Abuse Detection System (FADS) tool used to compare providers or recipients of the same peer group and detect potential fraud	
Provider Electronic Solutions (PES)	Software for providers to electronically submit claims and eligibility transactions to the Pennsylvania MMIS	
DXC Healthcare Provider Portal	Contractor licensed product that provides Internet functions, specifically ePrescribing for Pennsylvania	Limited to provider portal components implemented by the Department at the end of the Contract.
DXC Pennsylvania Account Wiki	Internal website used by Contractor staff for information sharing	Contractor internal use only and will not turned over to the Department at the end of the Contract.
FraudCapture®	Modular Web-based proprietary analytics platform designed to provide end-to-end support.	The FraudCapture Platform will not be turned over to the Department at the end of the Contract.

APPENDIX A-5-3

List of Third-Party Software and Tools in Use

The following is a list of the third-party software and tools used in support of the Pennsylvania MMIS and Fraud, Waste and Abuse Services. The vendor or manufacturer responsible for the software or the software license, its general function, version or model of the software, physical location, quantity, license owner, and comments explaining how it is used are shown below.

Because the vendor or manufacturer of this proprietary software is other than Contractor, Contractor will transfer the license when possible, in accordance with the license terms and conditions, or the Commonwealth will procure the necessary licenses to continue the full operation of the MMIS and Fraud, Abuse and Waste Services at the conclusion or termination of this Contract.

Legend: MDC=Mid Atlantic Data Center

Software Vendor	Function	Model or Type	Physical Location	Qty	License Owner	License Expire Date	Comments
Open Source							
	Programming language	PERL	MDC	3	Contractor	None	Free Open Source license
	HTTP/SOAP server	Apache 2	MDC	1	Contractor	None	Free Open Source license
Adobe							
	PDF file viewer	Acrobat Reader *5*	MDC	999	N/A	None	Free Adobe license
BCL Technologies	PDF File Creator	EasyPDF SDK	MDC	1	Contractor	Annual	One-time license purchase, annual maintenance fees
Checkpoint							
	Firewall software	NG-AI, R77, CPES-SS	MDC	1	Contractor	Annual	One-time license purchase, annual maintenance fees
	Firewall software	NG-AI, R77, CPES-SS	MDC	1	Contractor	Annual	One-time license purchase, annual maintenance fees
Computer Associates							
	Data Modeling	Erwin 4.1.4.4033	MDC	1	Contractor	None	Contractor Corporate license
	Problem tracking and Reporting	CA Unicenter Service Desk Build GA6022	MDC	1	Contractor	None	Contractor Corporate license
	Unix Job Scheduling	Autosys Rlse 3.5	MDC	2	Contractor	None	Contractor Corporate license
	Unix Job Scheduling	Autosys Rlse 3.5	MDC	1	Contractor	None	Contractor Corporate license
	Unix Job Scheduling	Autosys Rise 4.51	MDC	1	Contractor	None	Contractor Corporate license

DotNetNuke	Application Development	DotNetNuke	MDC	1	Contractor	Annual	One-time license purchase, annual maintenance fees
First DataBank							
	Drug Pricing	Drug pricing information	MDC	1	Contractor	Annual	
Impressions Technology							
	Scanning and OCR	ICapture IEditor V2.0	MDC	80	Contractor	Annual	One-time license purchase, annual maintenance fees
	Scanning application management	ICapture IQ Monitor V2.0	MDC	2	Contractor	Annual	One-time license purchase, annual maintenance fees
	Data entry reporting	ICapture IST AT Viewer V2.0	MDC	1	Contractor	Annual	One-time license purchase, annual maintenance fees
Intervoice Brite							
	AVRS system	Intervoice AYR system V3.2.l	MDC	3	Contractor	Annual	One-time license purchase, annual maintenance fees
	AVRS system reporting	Intervoice AVR reporting V3.2.l	MDC	3	Contractor	Annual	One-time license purchase, annual maintenance fees
L-Soft							

Software Vendor	Function	Model or Type	Physical Location	Qty	License Owner	License Expire Date	Comments
	eBulletin application	Listserv Maestro Enterprise Edition	MDC	1	Contractor	Annual	One-time license purchase, annual maintenance fees
Change Healthcare Solutions							
	Claim Check server software	MIM-McKesson Integration Module	MDC	1	Contractor	Annual	One-time license purchase, annual maintenance fees
	Claim Check GUI	Voyager2000 Wizard	MDC	1	Contractor	Annual	One-time license purchase, annual maintenance fees

	Claim Check	ClaimCheck	MDC	1	Contractor	Annual	One-time license purchase, annual maintenance fees
Micro Focus							
	Test Automation Software	UFT	MDC	3	Contractor	None	One-time license purchase, annual maintenance fees
Microsoft							
	Server Operating System	Widows Server 2003	MDC	2	Contractor	Annual	Contractor Corporate License
	Server Operating System	Windows Server 2008 R2	MDC	16	Contractor	Annual	Contractor Corporate License
	Server Operating System	Windows Server 2016 Data Center	MDC	144	Contractor	Annual	Contractor Corporate License
	Application Database	Microsoft SQL Server 2008 R2	MDC	4	Contractor	Annual	Contractor Corporate License
	Application Database	Microsoft SQL Server 2016	MDC	16	Contractor	Annual	Contractor Corporate License
	Application Development	Visual Studio .NET	MDC	10	Contractor	None	Contractor Corporate License
	General Office Applications	Microsoft 365	Account	200	Contractor	None	Contractor Corporate License
	Project Management	Microsoft Project	Camp Hill	20	Contractor	None	Contractor Corporate License
	Application	SharePoint (PROD)	MDC	1	Contractor	Monthly	SPLA licenses based on the hardware
	Application	SharePoint (non-PROD)	MDC	1	Contractor	Annual	One-time license purchase, annual maintenance fees

Software Vendor	Function	Model or Type	Physical Location	Qty	License Owner	License Expire Date	Comments
	Technical Drawings	Microso ft Visio	Camp Hill	10	Contractor	None	Contractor Corporate License
Nintex	Workflow and Reporting	K2 blackpearl	MDC	1	Contractor	Annual	One-time license purchase, annual maintenance fees
Open Source							
	Secure communications	CURL	MDC	1	Contractor	None	Open Source license agreement
OptiTech							
	Data Sort program	OT-Sort Rlse 1	MDC	2	Contractor	None	
Oracle							
	Oracle	Red Hat Linux CPU	MDC	40	Contractor	Annual	One-time license purchase, annual maintenance fees
	12.1 Enterprise	Sun SPARC CPU	MDC	24	Contractor	Annual	One-time license purchase, annual maintenance fees
	edition	Sun SPARC CPU	MDC	40	Contractor	Annual	One-time license purchase, annual maintenance fees
	Oracle 12.1	Package ofl0 Oracle Programmer Developer licenses	MDC	2	Contractor	Annual	One-time license purchase, annual maintenance fees
	Developer license	Oracle SQL Developer	MDC	999	*NIA*	None	

Software Vendor	Function	Model or Type	Physical Location	Qty	License Owner	License Expire Date	Comments
	Oracle 12.1 database Query	Oracle SQL PLUS	MDC	999	N/A	None	
	Oracle 12.1 database performance tuning	Oracle Diagnostic Tools	MDC	24	Contractor	Annual	One-time license purchase, annual maintenance fees
	Oracle 12.1 full client	Oracle Diagnostic Tools	MDC	6	Contractor	Annual	One-time license purchase, annual maintenance fees
	Unix Operating system	Solaris 10	MDC	3	Contractor	Annual	No cost license, annual maintenance fees
SAP							
	Database Analysis and Reporting Application	Business Objects V 6.5	MDC	1	Contractor	None	One-time license purchase, annual maintenance fees
	Designer	Business Objects V 6.5	MDC	1	Contractor	None	One-time license purchase, annual maintenance fees
	Web interface	Web Intelligence V 6.5	MDC	1	Contractor	None	One-time license purchase, annual maintenance fees
SwishZone							
	Web-based training development	SWISHrnax Build 2006.06.29	Camp Hill	1	Contractor	None	

Software Vendor	Function	Model or Type	Physical Location	Qty	License Owner	License Expire Date	Comments
TechSmith							
	Web-based training development	SnaglT 8.2	Camp Hill	1	Contractor	None	Shareware
Verisign							
	Web Server Security for Business Objects web server	Verisign SSL certificate	Camp Hill	1	Contractor	Annual	One-time license purchase, annual maintenance fees
	PROMIS*e*™ Internet web server	Verisign SSL certificate	Camp Hill	1	DHS	None	Certificate provided to Contractor under DHS/Commonwealth license with Verisign
VMWare							
	Virtual Machine Operating environment	ESXi 6.0	MDC	12	Contractor	Annual	One-time license purchase, annual maintenance fees
	Dynamic Resource Scheduling	DRS	Camp Hill	1	Contractor	None	Included in the Enterprise Edition

Software Vendor	Function	Model or Type	Physical Location	Qty	License Owner	License Expire Date	Comments
Appeon							
	Desktop Application	PowerBuilder Enterprise	Camp Hill	5	Contractor	Annual	Annual Subscription renewal
Checkpoint	Firewall software	CPAP-SG4800-NGFW-HA	Camp Hill	1	Contractor	Annual	One-time license purchase, annual maintenance fees
	Firewall software	CPAP-SG4800-NGFW	Camp Hill	1	Contractor	Annual	One-time license purchase, annual maintenance fees
	Firewall software	VPN	Camp Hill	200	Contractor	Annual	One-time license purchase, annual maintenance fees
Crawford Technologies	Application Development	CCM Gateway for Sharepoint (PROD)	MDC	1	Contractor	Annual	One-time license purchase, annual maintenance fees
	Application Development	CCM Gateway for Sharepoint (non-PROD)	MDC	1	Contractor	Annual	One-time license purchase, annual maintenance fees
	Application Development	CCM Gateway Developer	MDC	1	Contractor	Annual	One-time license purchase, annual maintenance fees
Citrix	Application Environment	Citrix Virtual Apps Premium	MDC	25	Contractor	Annual	One-time license purchase, annual maintenance fees
Microsoft	Server Operating System	Windows Server 2016	MDC	112	Contractor	Monthly	SPLA licenses based on the hardware
	Server Operating System	Windows Server 2016	Camp Hill	16	Contractor	Monthly	SPLA licenses based on the hardware
	Application Database	Microsoft SQL Server 2016	MDC	16	Contractor	Monthly	SPLA licenses based on the hardware
	Application Database	Microsoft SQL Server 2016	Camp Hill	1	Contractor	Monthly	SPLA licenses based on the hardware
Red Hat							
	Server Operating System	Red Hat Enterprise Linux Server Version 6.10	Camp Hill	2	Contractor	Annual	One-time license purchase, annual maintenance fees
	Server Operating System	Red Hat Enterprise Linux Server Version 6.10	MDC	6	Contractor	Annual	One-time license purchase, annual maintenance fees
	Server Operating System	Red Hat Enterprise Linux Server Version 7	MDC	2	Contractor	Annual	One-time license purchase, annual maintenance fees
	Support	Red Hat JBoss Enterprise Application Platform	N/A	1	Contractor	Annual	One-time license purchase, annual renewal

Software Vendor	Function	Model or Type	Physical Location	Qty	License Owner	License Expire Date	Comments
	Data Modeling	Erwin 4.1.4.4033	MDC	1	Contractor	None	Contractor Corporate license
	Problem tracking and Reporting	CA Unicenter Service Desk Build GA6022	MDC	1	Contractor	None	Contractor Corporate license
	Unix Job Scheduling	Autosys Rlse 3.5	MDC	2	Contractor	None	Contractor Corporate license
	Unix Job Scheduling	Autosys Rlse 3.5	MDC	1	Contractor	None	Contractor Corporate license
	Unix Job Scheduling	Autosys Rise 4.51	MDC	1	Contractor	None	Contractor Corporate license
First DataBank							
	Drug Pricing	Drug pricing information	MDC	1	Contractor	Annual	
Impressions Technology							
	Scanning and OCR	ICapture IEditor V2.0	MDC	80	Contractor	Annual	One-time license purchase, annual maintenance fees
	Scanning application management	ICapture IQ Monitor V2.0	MDC	2	Contractor	Annual	One-time license purchase, annual maintenance fees
	Data entry reporting	ICapture IST AT Viewer V2.0	MDC	1	Contractor	Annual	One-time license purchase, annual maintenance fees
Intervoice Brite							
	AVRS system	Intervoice AYR system V3.2.l	MDC	3	Contractor	Annual	One-time license purchase, annual maintenance fees
	AVRS system reporting	Intervoice AVR reporting V3.2.l	MDC	3	Contractor	Annual	One-time license purchase, annual maintenance fees
LISTSERV							

Software Vendor	Function	Model or Type	Physical Location	Qty	License Owner	License Expire Date	Comments
	Listserv	eBulletin application	MDC	1	Contractor	Annual	One-time license purchase, annual maintenance fees
McKesson							
	Claim Check server software	MIM– McKesson Integration Module	MDC	1	Contractor	Annual	One-time license purchase, annual maintenance fees
	Claim Check GUI	Voyager2000 Wizard	MDC	1	Contractor	Annual	One-time license purchase, annual maintenance fees
	Claim Check	ClaimCheck 8.5	MDC	1	Contractor	Annual	One-time license purchase, annual maintenance fees
Microsoft							
	Server Operating System	Widows Server 2003	MDC	4	Contractor	Annual	Contractor Corporate License
	Server Operating System	Windows Server 2008 R2	MDC	200	Contractor	Annual	Contractor Corporate License
	Application Database	Microsoft SQL Server 2008 R2	MDC	4	Contractor	Annual	Contractor Corporate License
	Application Development	Visual Studio .NET Version 7	MDC	10	Contractor	None	Contractor Corporate License
	Small-scale Database	Microsoft Access database, Rles 2000, 2002, 2003	MDC	60	Contractor	None	Contractor Corporate License
	General Project Support	Microsoft Office	Camp Hill	175	Contractor	None	Contractor Corporate License
	Email	Microsoft Outlook	Camp Hill	150	Contractor	None	Contractor Corporate License
	Project Management	Microsoft Project	Camp Hill	20	Contractor	None	Contractor Corporate License

Software Vendor	Function	Model or Type	Physical Location	Qty	License Owner	License Expire Date	Comments
	Technical Drawings	Microso ft Visio	Camp Hill	10	Contractor	None	Contractor Corporate License
Open Source							
	Secure communications	CURL	MDC	1	Contractor	None	Open Source license agreement
OptiTech							
	Data Sort program	OT-Sort Rlse 1	MDC	2	Contractor	None	
Oracle							
	Oracle	Red Hat Linux CPU	MDC	40	Contractor	Annual	One-time license purchase, annual maintenance fees
	12.1 Enterprise	Sun SPARC CPU	MDC	24	Contractor	Annual	One-time license purchase, annual maintenance fees
	edition	Sun SPARC CPU	MDC	40	Contractor	Annual	One-time license purchase, annual maintenance fees
	Oracle 12.1	Package ofl0 Oracle Programmer Developer licenses	MDC	2	Contractor	Annual	One-time license purchase, annual maintenance fees
	Developer license	Oracle SQL Developer	MDC	999	*NIA*	None	

Software Vendor	Function	Model or Type	Physical Location	Qty	License Owner	License Expire Date	Comments
	Oracle 12.1 database Query	Oracle SQL PLUS	MDC	999	N/A	None	
	Oracle 12.1 database performance tuning	Oracle Diagnostic Tools	MDC	24	Contractor	Annual	One-time license purchase, annual maintenance fees
	Oracle 12.1 full client	Oracle Diagnostic Tools	MDC	6	Contractor	Annual	One-time license purchase, annual maintenance fees
	Unix Operating system	Solaris 10	MDC	3	Contractor	Annual	No cost license, annual maintenance fees
SAP							
	Database Analysis and Reporting Application	Business Objects V 6.5	MDC	1	Contractor	None	One-time license purchase, annual maintenance fees
	Designer	Business Objects V 6.5	MDC	1	Contractor	None	One-time license purchase, annual maintenance fees
	Web interface	Web Intelligence V 6.5	MDC	1	Contractor	None	One-time license purchase, annual maintenance fees
SwishZone							
	Web-based training development	SWISHrnax Build 2006.06.29	Camp Hill	1	Contractor	None	

Software Vendor	Function	Model or Type	Physical Location	Qty	License Owner	License Expire Date	Comments
TechSmith							
	Web-based training development	SnaglT 8.2	Camp Hill	1	Contractor	None	Shareware
Unisys							
	Paper imaging and Workflow Application	UeWI (Unisys Infolimage e-Workflow& Imaging	MDC	1	Unisys	None	Proprietary to Unisys
Verisign							
	Web Server Security for Business Objects web server	Verisign SSL certificate	Camp Hill	1	Contractor	Annual	One-time license purchase, annual maintenance fees
	PROMIS*e*™ Internet web server	Verisign SSL certificate	Camp Hill	1	DHS	None	Certificate provided to Contractor under DHS/Commonwealth license with Verisign
VMWare							
	Virtual Machine Operating environment	ESXi 6.5	MDC	12	Contractor	Annual	One-time license purchase, annual maintenance fees
	Virtual Machine Management software	Virtual Center Server 2	MDC	1	Contractor	Annual	One-time license purchase, annual maintenance fees
	Dynamic Resource Scheduling	DRS	Camp Hill	1	Contractor	None	Included in the Enterprise Edition
American Medical Association							
	Current Procedural Terminology	N/A	FraudCaputre Platform	1	Contractor	None	Proprietary to the American Medical Association
OptumInsights, Inc.							
	Episode Treatment Group/Procedure Quality Measuremen	N/A	FraudCapture Platform	1	Contractor	05/2026	Proprietary to OptumInsights, Inc.

APPENDIX F

Requirements for Non-Commonwealth Hosted Applications/Services

The purpose of this Appendix F is to define requirements for technology solutions procured by the Commonwealth that are not hosted within Commonwealth infrastructure.

A. Hosting Requirements.

1. The Contractor and its subcontractor shall supply all hosting equipment (hardware and software) required for the cloud services and performance of the software and services set forth in the Contract.

2. The Contractor shall provide secure access to applicable levels of users via the internet.

3. The Contractor shall use commercially reasonable resources and efforts to maintain adequate internet connection bandwidth and server capacity
4. The Contractor and its subcontractors shall maintain all hosting equipment (hardware and software) required for cloud services and performance of software and services as set forth in the Contract and as required to maintain compliance with the Performance Requirements.

5. The Contractor shall monitor, prevent and deter unauthorized system access. Any and all known attempts must be reported to the Commonwealth within **48 hours**. Attempts do not include pings, broadcast attacks on firewalls, port scans, or denials of service ("Alerts") or any combination of Alerts unless such Alerts demonstrate a pattern of improper attempts or are targeted Alerts to access the system or if the Alerts exceed more than 20% of the normal volume of such Alerts. In the event of any impermissible disclosure, unauthorized loss or destruction of Confidential Information, the receiving Party must immediately notify the disclosing Party and take all reasonable steps to mitigate any potential harm or further disclosure of such Confidential Information. In addition, pertaining to the unauthorized access, use, release, or disclosure of data, the Contractor shall comply with state and federal data breach notification statutes and regulations, and shall report security incidents to the Commonwealth within **one hour** of when the Contractor has reasonable confirmation of such unauthorized access, use, release, or disclosure of data.

6. The Contractor and the Contractor's subcontractor shall allow the Commonwealth or its delegate, at times chosen by the Commonwealth, and within at least **three business days'** notice and in accordance with the cloud service provider's pre-existing policies and procedures, to review the hosted system's data center locations and security architecture.

7. The Contractor's employees and subcontractors, who are directly responsible for day-to-day monitoring and maintenance of the hosted system, shall have industry standard certifications applicable to the environment and system architecture used.

8. The Contractor and the Contractor's subcontractor shall locate servers in a climate-controlled environment. The Contractor or the Contractor's contractor shall house all servers and equipment in an operational environment that meets industry standards including climate control, fire and security hazard detection, electrical needs, and physical security.

9. The Contractor shall examine applicable system and error logs daily to minimize and predict system problems and initiate appropriate action.

10. The Contractor shall completely test and apply patches for all third-party software products in the server environment before release.

11. The Contractor shall comply with Attachment G, Framework for Independent Third-Party Security and Privacy Assessment Guidelines for Medicaid Enterprise Systems (MES) and Attachment 1, SOC Reporting Requirements.

12. The Contractor shall provide all Commonwealth data to the Commonwealth, upon request, in a form acceptable to the Commonwealth, at no cost to the Commonwealth.

B. **Security Requirements**.

1. The Contractor shall conduct a third-party independent security and vulnerability assessment at its own expense on an annual basis.

2. The Contractor shall comply with the Commonwealth's directions and resolutions to remediate the results of the security and vulnerability assessment to align with the standards of the Commonwealth.

3. The Contractor shall use industry best practices to protect access to the system with a firewall and firewall rules to prevent access by non-authorized users and block all improper and unauthorized access attempts.

4. The Contractor shall use industry best practices to provide applicable system intrusion detection and prevention in order to detect intrusions in a timely manner.

5. The Contractor shall use industry best practices to provide applicable malware and virus protection on all servers and network components.

6. The Contractor shall limit access to Commonwealth-specific systems, data and services and provide access only to those staff, located in the United States, that must have access to provide services proposed.

7. The Contractor shall provide the Services, using security technologies and techniques in accordance with industry best practices and the Commonwealth's ITPs set forth in Attachment 2, including those relating to the prevention and detection of intrusions, and any other inappropriate use or access of systems and networks.

C. Data Storage.

1. The Contractor shall store all Commonwealth data in the United States.

2. The Contractor shall use industry best practices to update and patch all applicable systems and third-party software security configurations to reduce security risk. The Contractor shall protect their operational systems with applicable anti-virus, host intrusion protection, incident response monitoring and reporting, network firewalls, application firewalls, and employ system and application patch management to protect its network and customer data from unauthorized disclosure.

3. The Contractor shall be solely responsible for applicable data storage required.

4. The Contractor shall encrypt all Commonwealth data in transit and at rest. The Contractor shall comply with ITP-SEC031, and ITP-SEC019, encryption policies and minimum standards or stronger.

5. The Contractor shall take all commercially viable and applicable measures to protect the data including, but not limited to, the backup of the servers on a daily basis in accordance with industry best practices and encryption techniques.

6. The Contractor shall have appropriate controls in place to protect critical or sensitive data and shall employ stringent policies, procedures, to protect that data particularly in instances where such critical or sensitive data may be stored on a Contractor-controlled or a Contractor-owned electronic device.

7. The Contractor shall utilize a secured backup solution to prevent loss of data, back up all data every day and store backup media. Stored backup media must be kept in an all-hazards protective storage safe at the worksite and when taken offsite. All back up data and media shall be encrypted.

D. Adherence to Policy.

1. The Contractor's support and problem resolution solution shall provide a means to classify problems as to criticality and impact and with appropriate resolution procedures and escalation process for classification of each problem.

2. The Contractor shall abide by the applicable Commonwealth's Information Technology Policies (ITPs), a list of the most relevant being attached hereto as Attachment 2.

3. The Contractor shall comply with all pertinent federal and state privacy regulations. Substantive changes to federal and state privacy regulations effective after the Effective Date of Amendment 7 will be addressed in accordance with Appendix A, Pennsylvania MMIS Terms and Conditions Section A-8.21 Compliance with Laws. Contractor will make reasonable efforts to investigate the impact of any change on the price, timetable, specifications, and other terms and conditions of the Contract. If the Commonwealth and the Contractor agree on the results of the investigation and any necessary changes to the Contract, the parties must complete and execute a change order to modify the Contract. If the parties are not able to agree upon the results of the investigation or the necessary changes to the Contract, a Commonwealth-initiated change request will be implemented at Commonwealth's option and the Contractor shall perform the Services; and either party may elect to have the matter treated as a Contract Controversies under Appendix A, Pennsylvania MMIS Terms and Conditions, Section A-8.13 Contract Controversies.

E. Closeout.

When the Contract term expires or terminates, and a new purchase order or other procurement document has not been issued by the Department within **60 days** of expiration or termination of the services to which these requirements apply, or as otherwise requirement under the Contract, the Contractor must promptly return to the Commonwealth all Commonwealth's data (and all copies of this information) that is in the Contractor's possession or control in accordance with the Contract. The Commonwealth's data shall be returned in a format agreed to by the Commonwealth and Contractor or as otherwise required under the Contract.

ATTACHMENT 1

SOC Reporting Requirements

(a) Subject to this section and unless otherwise agreed to in writing by the Commonwealth, the Contractor shall, and shall require its subcontractors to engage, on an annual basis, a CPA certified third-party auditing firm to the following, as applicable:

(i) a SOC 1 Type II report with respect to controls used by the Contractor relevant to internal and external procedures and systems that process Commonwealth financial transactions; and

(ii) a SOC 2 Type II report with respect to controls used by the Contractor relevant to internal and external procedures and systems that access, process, host or contain Commonwealth Data designated as Class "C" Classified Records or Closed Records, as defined in ITP-SEC019, or in compliance with mandates by federal or state audit requirements and/or policy.

Unless otherwise agreed to in writing by the Commonwealth, SOC Reports shall be provided upon contract execution and annually thereafter. While it is preferable that SOC Reports coincide with Pennsylvania's fiscal year (July 1 through June 30), SOC Reports, at the very least, must cover at least 6 consecutive months of Pennsylvania's fiscal year.

(b) SOC 2 Type II report reports shall address the following:

(i) Security of Information and Systems;

(ii) Availability of Information and Systems;

(iii) Processing Integrity;

(iv) Confidentiality;

(v) Privacy; and

(vi) If applicable, compliance with the laws, regulations standards or policies designed to protect the information identified in ITP-SEC019 or other information identified as protected or Confidential by this Contract or under law.

(c) At the request of the Commonwealth, the Contractor shall complete a SOC for Cybersecurity audit in the event:

(i) repeated non-conformities are identified in any SOC report required by subsection (a); or

(ii) if the Contractor's business model changes (such as a merger, acquisition, or change sub-contractors, etc.).

The SOC for Cybersecurity report shall detail the controls used by the Contractor setting forth the description and effectiveness of Contractor's cybersecurity risk management program and the policies, processes and controls enacted to achieve each cybersecurity objective.

The Contractor shall provide to the Commonwealth a report of the SOC for Cybersecurity audit findings within **60 days** of its completion.

(d) In addition to Appendix G, Framework for Independent Third-Party Security and Privacy Assessment Guidelines for Medicaid Enterprise Systems (MES) and this Attachment 1, the Commonwealth may specify other or additional standards, certifications or audits it requires under the Contract or within an ITP. Other or additional standards, certifications or audits effective after the Effective Date of Amendment 7 will be addressed in accordance with Appendix A, Pennsylvania MMIS Terms and Conditions Section A-7.2 Information Technology Standards. Contractor will determine any incremental costs resulting from such change. If the Commonwealth and the Contractor agree on the results of the costs, the parties will execute a change order to modify the Contract. If the parties are not able to agree upon the results of the investigation or the necessary changes to the Contract, a Commonwealth-initiated change request will be implemented at Commonwealth's option and the Contractor shall comply with the other or additional standard, certification or audit requirement and either party may elect to have the matter treated as a Contract Controversies under Appendix A, Pennsylvania MMIS Terms and Conditions, Section A-8.13 Contract Controversies.

(e) The Contractor shall adhere to SSAE 18 audit standards. The Contractor acknowledges that the SSAE guidance may be updated during the Term of this Contract, and the Contractor shall comply with such updates which shall be reflected in the next annual report.

(f) If an audit reveals any non-conformity to SSAE standards, the Contractor shall provide the Commonwealth, within **45 days** of the issuance of the SOC report, a documented corrective action plan that addresses each non-conformity. The corrective action plan shall provide, in detail:

(i) clear responsibilities of the personnel designated to resolve the non-conformity;

(ii) the remedial action to be taken by the Contractor or its subcontractor(s);

(iii) the dates when each remedial action is to be implemented; and

(iv) a summary of potential risks or impacts to the Commonwealth that are associated with the non-conformity(ies).

(g) The Commonwealth may in its sole discretion agree, in writing, to accept alternative and equivalent reports or certifications in lieu of a SOC report.

ATTACHMENT 2

Information Technology Policies (ITPs)

ITP Number - Name	Policy Link
ITP_ACC001 - Accessibility Policy	https://www.oa.pa.gov/Policies/Documents/itp_acc001.pdf
ITP_APP030 - Active Directory Architecture	https://www.oa.pa.gov/Policies/Documents/itp_app030.pdf
ITP_BUS007 - Enterprise Service Catalog	https://www.oa.pa.gov/Policies/Documents/itp_bus007.pdf
ITP_BUS010 - Business Process Management Policy	https://www.oa.pa.gov/Policies/Documents/itp_bus010.pdf
ITP_BUS012 -Artificial Intelligence General Policy	httpss://www.oa.pa.gov/Policies/Documents/itp_bus012.pdf
ITP_INF000 - Enterprise Data and Information Management Policy	https://www.oa.pa.gov/Policies/Documents/itp_inf000.pdf
ITP_INF001 - Database Management Systems	https://www.oa.pa.gov/Policies/Documents/itp_inf001.pdf
ITP_INF006 - Commonwealth County Code Standard	https://www.oa.pa.gov/Policies/Documents/itp_inf006.pdf
ITP_INF009 - e-Discovery Technology Standard	https://www.oa.pa.gov/Policies/Documents/itp_inf009.pdf
ITP_INF010 - Business Intelligence Policy	https://www.oa.pa.gov/Policies/Documents/itp_inf010.pdf
ITP_INF011 - Reporting Policy	https://www.oa.pa.gov/Policies/Documents/itp_inf011.pdf
ITP_INF012 - Dashboard Policy	https://www.oa.pa.gov/Policies/Documents/itp_inf012.pdf
ITP_INFRM001 - The Life Cycle of Records: General Policy Statement	https://www.oa.pa.gov/Policies/Documents/itp_infrm001.pdf
ITP_INFRM004 - Management of Web Records	https://www.oa.pa.gov/Policies/Documents/itp_infrm004.pdf
ITP_INFRM005 - System Design Review of Electronic Systems	https://www.oa.pa.gov/Policies/Documents/itp_infrm005.pdf
ITP_INFRM006 - Electronic Document Management Systems	https://www.oa.pa.gov/Policies/Documents/itp_infrm006.pdf
ITP_INT_B_1 - Electronic Commerce Formats and Standards	https://www.oa.pa.gov/Policies/Documents/itp_int_b_1.pdf
ITP_INT_B_2 - Electronic Commerce Interface Guidelines	https://www.oa.pa.gov/Policies/Documents/itp_int_b_2.pdf
ITP_INT006 - Business Engine Rules	https://www.oa.pa.gov/Policies/Documents/itp_int006.pdf
ITP_NET004 - Internet Protocol Address Standards	https://www.oa.pa.gov/Policies/Documents/itp_net004.pdf
ITP_NET005 - Commonwealth External and Internal Domain Name Services (DNS)	https://www.oa.pa.gov/Policies/Documents/itp_net005.pdf
ITP_PRV001 - Commonwealth of Pennsylvania Electronic Information Privacy Policy	https://www.oa.pa.gov/Policies/Documents/itp_prv001.pdf
ITP_SEC000 - Information Security Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec000.pdf
ITP_SEC001 - Enterprise Host Security Software Policy	httpss://www.oa.pa.gov/Policies/Documents/itp_sec001.pdf
ITP_SEC002 - Internet Accessible Proxy Servers and Services	https://www.oa.pa.gov/Policies/Documents/itp_sec002.pdf
ITP_SEC003 - Enterprise Security Auditing and Monitoring	https://www.oa.pa.gov/Policies/Documents/itp_sec003.pdf
ITP_SEC004 - Enterprise Web Application Firewall	https://www.oa.pa.gov/Policies/Documents/itp_sec004.pdf
ITP_SEC006 - Commonwealth of Pennsylvania Electronic Signature Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec006.pdf
ITP_SEC007 - Minimum Standards for IDs, Passwords and Multi-Factor Authentication	https://www.oa.pa.gov/Policies/Documents/itp_sec007.pdf
ITP_SEC008 - Enterprise E-mail Encryption	https://www.oa.pa.gov/Policies/Documents/itp_sec008.pdf
ITP_SEC009 - Minimum Contractor Background Checks Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec009.pdf
ITP_SEC010 - Virtual Private Network Standards	https://www.oa.pa.gov/Policies/Documents/itp_sec010.pdf

ITP Number - Name	Policy Link
ITP_SEC011 - Enterprise Policy and Software Standards for Agency Firewalls	https://www.oa.pa.gov/Policies/Documents/itp_sec011.pdf
ITP_SEC012 - System Logon Banner and Screensaver Requirements	httpss://www.oa.pa.gov/Policies/Documents/itp_sec012.pdf
ITP_SEC015 - Data Cleansing	https://www.oa.pa.gov/Policies/Documents/itp_sec015.pdf
ITP_SEC016 - Information Security Officer Policy	httpss://www.oa.pa.gov/Policies/Documents/itp_sec016.pdf
ITP_SEC017 - Copa Policy for Credit Card Use for e-Government	https://www.oa.pa.gov/Policies/Documents/itp_sec017.pdf
ITP_SEC019 - Policy and Procedures for Protecting Commonwealth Electronic Data	https://www.oa.pa.gov/Policies/Documents/itp_sec019.pdf
ITP_SEC021 - Security Information and Event Management Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec021.pdf
ITP_SEC023 - Information Technology Security Assessment and Testing Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec023.pdf
ITP_SEC024 - IT Security Incident Reporting Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec024.pdf
ITP_SEC025 - Proper Use and Disclosure of Personally Identifiable Information (PII)	https://www.oa.pa.gov/Policies/Documents/itp_sec025.pdf
ITP_SEC029 - Physical Security Policy for IT Resources	https://www.oa.pa.gov/Policies/Documents/itp_sec029.pdf
ITP_SEC031 - Encryption Standards	https://www.oa.pa.gov/Policies/Documents/itp_sec031.pdf
ITP_SEC032 - Enterprise Data Loss Prevention (DLP) Compliance Standards	https://www.oa.pa.gov/Policies/Documents/itp_sec032.pdf
ITP_SEC034- Enterprise Firewall Rule Set	https://www.oa.pa.gov/Policies/Documents/itp_sec034.pdf
ITP_SEC035 - Mobile Device Security Policy	httpss://www.oa.pa.gov/Policies/Documents/itp_sec035.pdf
ITP_SEC038 - Commonwealth Data Center Privileged User IAM Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec038.pdf
ITP-SEC039 - Keystone Login and Identity Proofing	https://www.oa.pa.gov/Policies/Documents/itp-sec039.pdf
ITP_SEC040 - Commonwealth Cloud Computing Services Requirements	https://www.oa.pa.gov/Policies/Documents/itp_sec040.pdf
ITP SFT000 - Software Development Life Cycle (SDLC) Policy	https://www.oa.pa.gov/Policies/Documents/itp_sft000.pdf
ITP_SFT001 - Software Licensing	https://www.oa.pa.gov/Policies/Documents/itp_sft001.pdf
ITP_SFT002 - Commonwealth of PA Website Standards	https://www.oa.pa.gov/Policies/Documents/itp_sft002.pdf
ITP_SFT003 - Geospatial Enterprise Service Architecture	https://www.oa.pa.gov/Policies/Documents/itp_sft003.pdf
ITP_SFT004 - Geospatial Information Systems (GIS)	https://www.oa.pa.gov/Policies/Documents/itp_sft004.pdf
ITP_SFT005 - Managed File Transfer (MFT)	https://www.oa.pa.gov/Policies/Documents/itp_sft005.pdf
ITP_SFT007 - Office Productivity Policy	https://www.oa.pa.gov/Policies/Documents/itp_sft007.pdf
ITP SFT008 - Enterprise Resource Planning (ERP) Management	https://www.oa.pa.gov/Policies/Documents/itp_sft008.pdf
ITP SFT009 - Application Development	https://www.oa.pa.gov/Policies/Documents/itp_sft009.pdf
ITP_SYM003 - Off-Site Storage for Commonwealth Agencies	https://www.oa.pa.gov/Policies/Documents/itp_sym003.pdf
ITP_SYM004 - Policy for Establishing Alternate Processing Sites for Commonwealth Agencies	https://www.oa.pa.gov/Policies/Documents/itp_sym004.pdf
ITP_SYM006 - Commonwealth IT Resources Patching Policy	https://www.oa.pa.gov/Policies/Documents/itp_sym006.pdf
ITP_SYM008 - Server Virtualization Policy	https://www.oa.pa.gov/Policies/Documents/itp_sym008.pdf
ITP_SYM010 - Enterprise Services Maintenance Scheduling	https://www.oa.pa.gov/Policies/Documents/itp_sym010.pdf

Centers for Medicare & Medicaid Services

Framework for the Independent Third-Party Security and Privacy Assessment Guidelines for Medicaid Enterprise Systems (MES)

Final Draft

Version 1.0

January 14, 2020

Table of Contents

List of Tables

1. Introduction

The state Medicaid Enterprise System (MES) is the custodian of sensitive information, such as Personally Identifiable Information (PII) or Protected Health Information (PHI), for millions of individuals receiving coverage through Medicaid and the Children's Health Insurance Program (CHIP). The state and its business partners share the responsibility for ensuring the protection of this sensitive information. States and their respective business partners must demonstrate continuous monitoring and regular security and privacy control testing through an independent security and privacy assessment.

This guidance document provides an overview of the independent security and privacy assessment requirements.

1.1 Requirements Background

Pursuant to the Health Insurance Portability and Accountability Act (HIPAA) and implementing regulations at 45 CFR §164.308(a)(1)(ii)(A), conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications of HIPAA. Therefore, a risk analysis is foundational, and must be completed to assist organizations in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards of PHI/PII. Furthermore, the National Institute of Standards and Technology (NIST), Security Assessments Control, CA-2, requires an independent assessment of all applicable security and privacy controls. States should have a fully completed and implemented System Security/Privacy Plan (SSP) before starting the security and privacy assessment. CMS highly recommends an independent third-party assessor conduct the assessment.

1.2 Purpose

This guidance document provides an overview of the independent security and privacy assessment requirements through the following objectives:

- Define the independent third-party assessor (Section 2);
- Explain the scope of the security and privacy control assessment and provide assessment planning considerations (Section 3);
- Provide a basic security and privacy control assessment methodology (Section 4); and
- Summarize security and privacy assessment reporting (Section 5).

This document is not intended to provide detailed guidance for assessment planning and performance, nor for state planning and action to address assessment findings.

2. Independent Third-Party Security and Privacy Assessor

Pursuant to 45 CFR § 95.621(f) and consistent with State Medicaid Director Letter (SMDL) #06-022[1], CMS requires that state agencies employ assessors or assessment teams to conduct periodic

[1] Available at: https://downloads.cms.gov/cmsgov/archived-downloads/SMDL/downloads/SMD092006.pdf

security and privacy control assessments of the MES environment. The assessor's role is to provide an independent assessment of the effectiveness of implementations of security and privacy safeguards for the MES environment and to maintain the integrity of the assessment process.

2.1 Assessor Independence and Objectivity

An assessor must be free from any real or perceived conflicts of interest, including being free from personal, external, and organizational impairments to independence, or the appearance of such impairments to independence. An assessor is considered independent if there is no perceived or actual conflict of interest involving the developmental, operational, financial, and/or management chain associated with the system and the determination of security and privacy control effectiveness.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39, *Managing Information Security Risk*[2], states that:

> "Assessor independence is an important factor in: (i) preserving the impartial and unbiased nature of the assessment process; (ii) determining the credibility of the security assessment results; and (iii) ensuring that the authorizing official receives the most objective information possible in order to make an informed, risk-based, authorization decision."

2.2 Assessor Qualifications

Experience and competencies are important factors in selecting an assessor. CMS recommends that the MES assessor possess a combination of privacy and security experience and relevant assessment certifications. Examples of acceptable privacy and security experience include, but are not limited to:

- Reviewing compliance with HIPAA security standards;
- Reviewing compliance with the most current NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, or the most current NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*;
- Reviewing compliance with the Minimal Acceptable Risk Standards for Exchange (MARS-E);
- Reviewing compliance with the Federal Information Security Management Act (FISMA);
- Participating in the Federal Risk and Authorization Management Program (FedRAMP)-certified third-party assessment organization; and
- Reviewing compliance with the Statement on Standards for Attestation Engagements (SSAE) 16.

Examples of relevant auditing certifications are:

[2] Available at: https://csrc.nist.gov/publications/detail/sp/800-39/final

- Certified Information Privacy Professional (CIPP);
- Certified Information Privacy Manager (CIPM);
- Certified Information Systems Security Professional (CISSP);
- Fellow of Information Privacy (FIP);
- HealthCare Information Security and Privacy Practitioner (HCISPP);
- Certified Internal Auditor (CIA);
- Certified Risk Management Professional (CRMP);
- Certified Information Systems Auditor (CISA); or
- Certified Government Auditing Professional (CGAP).

2.3 Assessor Options

CMS strongly recommends the use of a third-party experienced security and privacy assessor. However, internal state staff may be leveraged, provided they have appropriate qualifications to evaluate the implementation of security and privacy controls. The internal state staff must be familiar with HIPAA regulations, NIST standards, and other applicable federal privacy and cybersecurity regulations and guidance. The internal state staff must also meet the assessor independence, objectivity, and qualifications as documented in Sections 2.1 and 2.2. Furthermore, the internal state staff must be capable of performing penetration testing and vulnerability scans.

3. Assessment Scope and Planning

3.1 Scope of the Independent Security and Privacy Control Assessment

The purpose of a Security Control Assessment (SCA) is to determine whether the security and privacy controls are implemented correctly, operate as intended, and produce the desired outcomes for meeting the security and privacy requirements of the application or system. The SCA also identifies areas of risk that require the state's attention and remediation. The independently conducted SCA provides an understanding of the following:

- The MES application or system's compliance with the state security and privacy control requirements;
- The underlying infrastructure's security posture;
- Any application and/or system security, data security, and privacy vulnerabilities to be remediated to improve the MES's security and privacy posture; and
- The state's adherence to its security and privacy program, policies, and guidance.

3.2 Vulnerabilities and Testing Scenarios

Given the sensitivity of data processed in the MES and the high threat of the web environment, it is critically important that the security of web applications deployed meet the present-day known security attack vectors and situations. The Open Web Application Security Project (OWASP)[3] keeps an up-to-date list that identifies such attacks and situations. In addition to the mandated security and privacy controls, the independent SCA requires penetration tests to determine vulnerabilities associated with known attacks and situations obtained from the current OWASP Top 10 – *The Ten Most Critical Web Application Security Risks*. The assessment should adjust the SCA scope to address current OWASP list of vulnerabilities. The state should regularly review the following list to determine the current vulnerabilities in the OWASP Top 10, including, but not limited to:

- Injection;
- Broken Authentication;
- Sensitive Data Exposure;
- XML External Entity (XXE);
- Broken Access Control;
- Security Misconfiguration;
- Cross-Site Scripting (XSS);
- Insecure Deserialization;
- Using Components with Known Vulnerabilities; and
- Insufficient Logging and Monitoring.

3.3 Assessment of Critical Security Controls

Test scenarios must adequately assess the implementation status of critical security controls identified by the Center for Internet Security (CIS).[4] The testing scenario information is available for each CIS control at the CIS site. The main testing points identified by the CIS are incorporated into the SCA scope, corresponding Security and Privacy Controls Assessment Test Plan (SAP), and testing criteria.

3.4 Assessment Planning

The state is encouraged to develop an assessment strategy and procedure that provides a standardized approach for planning and resourcing the SCA of its applications, systems, and underlying components. The state is responsible for ensuring that each SCA has:

- Budget and assigned resources suitable for completing the assessment;
- Clear objectives and constraints;
- Well-defined roles and responsibilities; and
- Scheduling that includes defined events and deliverables.

During planning for the SCA, the state develops a scope statement that is dependent on, but not limited to, the following factors:

- Application or system boundaries;

[3] Available at: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[4] CIS Top 20 Critical Controls, available at: https://www.cisecurity.org/controls/.

- Known business and system risks associated with the application or system;
- Dependence of the application or system on any hierarchical structure;
- Current application or system development phase; and
- Documented security and privacy control requirements.

The assessor's SCA contract statement of work should include requirements to provide support to clarify findings and make corrective action recommendations after the assessment. The contract terms should also specify that all assessor staff must execute Non-Disclosure Agreements (NDAs) before accessing any information related to the security and privacy of the application or system. Requests to access information should only be considered based on a demonstration of a valid need to know, and not a position, title, level of investigation, or position sensitivity level.

4. Security and Privacy Control Assessment Methodology

The SCA methodology described in this guidance originates from the standard CMS methodology used in the assessment of all CMS internal and business partner applications or systems.

Assessment procedures for testing each security and privacy control should be consistent with the methodology documented in the most current version of the NIST SP 800-53A[5], *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*. The assessor should prepare a detailed assessment plan using these security and privacy control assessment procedures, the main testing points for the CIS critical controls, and detailed directions for addressing the penetration testing procedures for the OWASP Top 10 vulnerabilities. The assessor should modify or supplement the procedures to evaluate the application's or system's vulnerability to different types of threats, including those from insiders, the Internet, or the network. The assessment methods should include examination of documentation, logs and configurations, interviews of personnel, and testing of technical controls. Control assessment procedures and associated test results provide information to identify the following:

- Application or system vulnerabilities, the associated business and system risks, and potential impact;
- Weaknesses in the configuration management process, such as weak system configuration settings that may compromise the Confidentiality, Integrity, and Availability (CIA) of the system;
- State and/or federal policies not followed; and
- Major documentation omissions and/or discrepancies.

4.1 Security and Privacy Control Technical Testing

To conduct security technical testing, the state grants assessor staff user access to the application or system. The state system administrator establishes application-specific user accounts for the assessor that reflect the different user types and roles. Through this access and these accounts,

[5] Available at: https://csrc.nist.gov/publications/detail/sp/800-53a/rev-4/final.

the assessor can perform a thorough assessment of the application or system and test application and system security controls that might otherwise not be tested. The assessor should not be given a user account with a role that would allow access to PHI/PII in any application or database.

The assessor should attempt to expose vulnerabilities associated with gaining unauthorized access to the application or system resources by selecting and employing tools and techniques that simulate vulnerabilities, such as buffer overflows and password compromises. The assessor must use caution to ensure against any inadvertent alteration of important settings that may disable or degrade essential security or business functions. Because many automated testing utilities mimic signs of attack and/or exploit vulnerabilities, the assessor must identify in the SAP all proposed tools that pose a risk to the computing environment. Furthermore, any testing that could potentially expose PHI/PII must be performed under the direct supervision of an authorized individual who is responsible for the data and can monitor the assessor's actions and take appropriate measures to protect any data that is vulnerable to exposure.

4.2 Network and Component Scanning

To gain an understanding of a network and component infrastructure security posture, the SCA includes network-based infrastructure scans, database scans, web application scans, and penetration tests for all in-scope components, applications, and systems. This scope provides a basis for determining the extent to which the security controls implemented within the network meet security control requirements. The assessor evaluates the results of these scans in conjunction with the configuration assessment.

4.3 Configuration Assessment

The performance of the configuration assessment provides the assessor with another mechanism for determining if the state's security requirements are implemented correctly in the application or system, or if the system environmental components are implemented correctly within the boundary of the application or system. The process for performing the configuration assessment requires the assessor to:

- Review the implemented configurations for each component against the state's security and privacy requirements;
- Review access to the system and databases for default user accounts;
- Test firewalls, routers, systems, and databases for default configurations and user accounts;
- Review firewall access control rules against the state's security requirements; and
- Determine consistency of system configuration with the state's documented configuration standards.

4.4 Documentation Review

The assessor should review all security and privacy documentation for completeness and accuracy and gain the necessary understanding to determine the security and privacy posture of the application or system. Through this process, the assessor develops insight into the documented security and privacy controls in place to effectively assess whether all controls are implemented as described. The documentation review augments all testing: it is an essential element for evaluating compliance of the documented controls versus the actual implementation as revealed during technical testing, scanning, configuration assessment, and personnel interviews.

For example, if the specified control stipulates that the password length for the system must be eight characters, the assessor must review the state's password policy or the SSP to verify compliance with this requirement. During the technical configuration assessment, the Assessor confirms passwords are configured as stated in the state's documentation. Table 1 identifies examples of core security documentation for review.

Table 1. Core Security and Privacy Documentation

NIST/State Control Family	NIST/State Control Number	Document Name
Planning (PL)	PL-2: System Security and Privacy Plan (SSP)	System Security and Privacy Plan (SSP)
Configuration Management (CM)	CM-9: Configuration Management Plan	Configuration Management Plan (CMP)
Contingency Planning (CP)	CP-2: Contingency Plan	Contingency Plan (CP)
Contingency Planning (CP)	CP-4: Contingency Plan Testing and Exercises	CP Test Plan and Results
Incident Response (IR)	IR-8: Incident Response Plan	Incident Response Plan (IRP)
Incident Response (IR)	IR-3: Incident Response Testing and Exercises	IRP Test Plan
Awareness and Training (AT)	AT-3: Security Training	Security Awareness Training Plan
Awareness and Training (AT)	AT-4: Security Training	Training Records
Security and Assessment Authorization (CA)	CA-3: System Interconnections	Interconnection Security Agreements (ISA)
Risk Assessment (RA)	RA-3: Risk Assessment	Information Security Risk Assessment (ISRA)
Authority and Purpose (AP)	AP-1: Authority to Collect	Privacy Impact Assessment (PIA) or other privacy documents
Authority and Purpose (AP)	AP-2: Purpose Specification	Privacy documents and notices including, but not limited to, PIAs and agreements to collect, use, and disclose PHI/PII and Privacy Act Statements
Accountability, Audit, and Risk Management (AR)	AR-1: Governance and Privacy Program	Governance documents and privacy policy
Accountability, Audit, and Risk Management (AR)	AR-2: Privacy Impact and Risk Assessment	Documentation describing the organization's privacy risk assessment process, documentation of privacy risk assessments performed by the organization

4.5 Personnel Interviews

The assessor conducts personnel interviews to validate the implementation of security and privacy controls, confirm that staff understand and follow documented control implementations, and verify the appropriate distribution of updated documentation to staff. The assessor interviews business, information technology, and support personnel to ensure effective implementation of operational and managerial security and privacy controls across all support areas. The assessor will customize interview questions to focus on control assessment procedures applicable to individual roles and responsibilities and assure that state staff are properly implementing and/or executing security and privacy controls.

The SCA test plan identifies the designated state subject matter experts (SME) to interview. These SMEs should have specific knowledge of overall security and privacy requirements and a detailed understanding of the application or system operational functions. The state staff selected for conducting interviews may have the following roles:

- Business Owner(s);
- Application Developer;
- Configuration Manager;
- Contingency Planning Manager;
- Database Administrator;
- Data Center Manager;
- Facilities Manager;
- Firewall Administrator;
- Human Resources Manager;
- Information System Security Officer;
- Privacy Program Manager;
- Privacy Officer;
- Media Custodian;
- Network Administrator;
- Program Manager;
- System Administrators;
- System Owner; and
- Training Manager.

Although the initial identification of interviewees is determined when the SAP is prepared, additional staff may be identified for interviewing during the SCA process.

4.6 Penetration Testing

At a minimum, penetration testing includes the tests found in subsection 3.2 (based on the OWASP Top 10). The *Security and Privacy Controls Assessment Test Plan* should properly document the tools, methods, and processes for penetration testing. The test plan should clearly account for and coordinate any special requirements or permissions for penetration testing during the SCA.

5. Security and Privacy Assessment Reporting

At the completion of the assessment, the assessor provides a Security and Privacy Assessment Report (SAR) to the state's Business Owner, who is then responsible for providing the report to CMS. The SAR's structure and content (as described in the following subsection) must be consistent with the assessment objectives. The SAR allows the assessor to communicate the assessment results to several audience levels, ranging from executives to technical staff.

The SAR is not a living document; findings should not be added and removed from the SAR.

5.1 SAR Content

The SAR content includes the following information:

- System Overview;
- Executive Summary Report;
- Detailed Findings Report;
- Scan Results
  - Infrastructure Scan
  - Database Scan
  - Web Applications Scan;
- Penetration Test Report; and
- Penetration Test and Scan Results Summary.

The SAR presents the results of all testing performed, including technical testing, scans, configuration assessment, documentation review, personnel interviews, and penetration testing. Results from multiple testing sources may be consolidated in one finding, if findings are closely related. The findings of the assessment should be annotated in detail with the remediation recommendations for the weaknesses and deficiencies found in the system security and privacy controls implementation. To reduce the risks posed to this important healthcare service and to protect the sensitive information of the citizens who use this service, the assessment team must assign business and system risk levels to each specific finding. The assignment of these risk levels should follow the methodology outlined in NIST SP 800-30 Rev. 1, Appendices G, H, and I[6] when assigning risk levels.

The SAR structure should allow the independent third-party assessor to communicate the security and privacy assessment results to several targeted audience levels, ranging from executives to technical staff. A sample SAR used by the Federal Risk and Authorization Management Program (FedRAMP) can be modeled after[7].

[6] NIST 800-30 Rev.1, Appendices G, H, and I. Available at: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

[7] FedRAMP SAR Template. Available at: https://www.fedramp.gov/templates/.

6. Summary

All organizations should perform either an internal risk assessment, or engage an industry recognized security privacy expert, to conduct an external risk assessment of the organization in order to identify and address security and privacy vulnerabilities. Information security and privacy safeguards and continuous monitoring are dynamic processes that must be effectively and proactively managed to support organizational risk management decisions. Independent security and privacy assessment provides a mechanism for the organization to identify and respond to new vulnerabilities, evolving threats, and a constantly changing enterprise architecture and operational environment, which can feature changes in hardware or software, as well as risks from the creation, collection, disclosure, access, maintenance, storage, and use of data. Through ongoing assessment and authorization, organization can detect changes to the security and privacy posture of an IT system, which is essential to making well-informed, risk-based decisions about the system within the MES.

Appendix H

FRAUDCAPTURE™ SERVICES SUPPLEMENT

This Supplement governs the Department's use of Gainwell's FraudCapture Platform only.

Except as set forth herein, all other terms and conditions of the FraudCapture SOW and any resulting Change Order and the Contract, as amended, remain in full force and effect.

SECTION 1. DEFINITIONS

1.1 **Department Data** means all Department provider data, claims data and other member related data used by Gainwell to populate the FraudCapture Platform.

1.2 **Documentation** means the user guide and release notes regarding use of the FraudCapture Platform that may be published by Gainwell from time to time.

1.3 **FraudCapture Platform** means Gainwell's modular Web-based proprietary analytics platform designed to provide end-to-end support for special investigative unit operations.

1.4 **FraudCapture Services** means Gainwell's provision of Department's access to and use of the Documentation, the FraudCapture Platform, and the outputs of the FraudCapture Platform

1.5 **User** means an individual who: (i) is an employee or contractor of Department; (ii) is authorized by Department to access and use the FraudCapture Platform pursuant to these terms; and (iii) has received User Credentials from Department or Gainwell.

1.6 **User Credentials** means the confidential and unique access details issued to a User to access and use the FraudCapture Platform in accordance with these terms.

SECTION 2. SUPPORT SERVICES

Support Services will be provided in accordance with the Contract and as defined more fully during implementation.

SECTION 3. GAINWELL OBLIGATIONS

3.1 General. Subject to compliance with these terms by Department and its Users, Gainwell agrees to provide Department and its Users access to the FraudCapture Platform using Department provided hardware and communication services via the Internet.

3.2 Implementation. Gainwell will implement access to the FraudCapture Platform for Department and its Users, including setup and management of User Credentials, in accordance with the implementation plan.

3.3 Training. Gainwell will provide training on the use of the FraudCapture Platform to Department and its Users in accordance with Section 9 of the SOW.

3.4 Database Population. Gainwell will populate the FraudCapture Platform with Department Data.

3.5 Modifications and Enhancements. Gainwell reserves the right to modify or enhance the FraudCapture Platform provided that no such modification or enhancement affects the functionality of the FraudCapture Platform in a materially adverse manner. Gainwell agrees to make available to Department any associated updates to the Documentation resulting from such modifications or enhancements.

SECTION 4. DOCUMENTATION AND DEPARTMENT ACCESS TO THE FRAUDCAPTURE PLATFORM

4.1 Use of Documentation. As reasonably necessary, Department may make and distribute copies of the Documentation in connection with its use of the FraudCapture Platform. However, Department must include on any Documentation copy all copyright and other proprietary notices as presented in the original Documentation.

4.2 Department and User Access to the FraudCapture Platform

4.2.1 Access to and use of the FraudCapture Platform is limited to Department and its Users. Gainwell grants to Department a limited, non-exclusive, non-sublicensable, revocable, and non-transferable license to access the FraudCapture Platform solely for Department's internal use in accordance with these terms. Department and its Users shall not attempt to perform or perform (and Department shall not permit a third party acting for the benefit of Department to perform) the following acts: (i) reverse-engineer, replicate, de-encrypt, or decompile any of the intellectual property platforms in the FraudCapture Platform or in any related Gainwell IP; (ii) modify, copy, or create derivative works based on the FraudCapture Platform;

(iii) remove, obscure or alter any copyright or proprietary notices associated with the Documentation or the FraudCapture Platform; or (iv) sell or sublicense access to and use of the FraudCapture Platform.

4.2.2 The FraudCapture Platform is and contains proprietary trade secrets and confidential information of Gainwell and its affiliate HMS, including but not limited to materials, processes and process flows, programs, software systems and documentation, information management systems, code, logic, analytical methodologies and algorithms, reports, analyses, data, associated proprietary forms of data organization and reports and other Gainwell intellectual property and the Department agrees to (i) to exercise the same care to protect Gainwell confidential information as it would to protect its own comparable confidential information, but in no event less than reasonable care; (ii) to use or disclose Gainwell confidential information only for the purposes of the Contract and will not disclose such Confidential Information to any third party without the Gainwell's prior written consent, other than to each other's authorized employees and officers, directors, contractors, advisors and agents on a need-to-know basis and who are bound by confidentiality obligations that are at least as protective as those contained in this Contract, and (iii) that in the event of a state or federal open records or freedom of information act request for disclosure of any confidential information related to or arising out of this Supplement, Department shall provide written notice to Gainwell to allow Gainwell the opportunity to respond to the open records or other freedom of information act requester and protect any proprietary trade secrets and confidential information

4.2.3 If there is a conflict between the online end-user access and use license language that is included as part of the FraudCapture Platform login screen or any content page of the FraudCapture Platform, the language of this Appendix H terms shall control.

4.3 Effect of Termination. Upon termination of Department's receipt of the FraudCapture Services: (a) all rights granted to Department under these terms will immediately terminate; (b) Department and its Users must cease access to the FraudCapture Platform; and (c) Department must destroy all copies of the Documentation in the possession of Department and any User.

SECTION 6. THIRD PARTY END USER AGREEMENTS

Third party mandatory flow-down terms and conditions are specified below:

A. AMA END USER AGREEMENT

The FraudCapture Platform incorporates the American Medical Association's ("AMA") Current Procedural Terminology® (CPT®) codes and descriptions ("**Editorial Content**") made available to Gainwell's affiliate, Health Management Systems, Inc. ("HMS"), under a license granted by the AMA. HMS is authorized by the AMA to distribute to and sublicense use of the Editorial Content to Gainwell, Department and its Users via use of the FraudCapture Platform subject to Department and its Users being bound by the AMA End User Terms.

Department on behalf of itself and its User agrees to the following AMA terms and conditions ("**AMA End User Terms**"):

1. Department's right to use the Editorial Content contained within the FraudCapture Platform is nontransferable, nonexclusive, and for the sole purpose of internal use by Department, and only within Algeria, Argentina, Australia, Bahamas, Belgium, Bermuda, Brazil, British Virgin Islands, Canada, Cayman Islands, Chile, China, Colombia, Costa Rica, Denmark, Dominican Republic, Ecuador, El Salvador, Finland, France, Germany, Guatemala, Hong Kong, India, Ireland, Israel, Italy, Jamaica, Japan, Jordan, Republic of Korea (South Korea), Lebanon, Mexico, New Zealand, Norway, Panama, Philippines, Portugal, Saudi Arabia, Singapore, South Africa, Spain, Sweden, Switzerland, Thailand, Turkey, United Arab Emirates, United Kingdom, United States and its territories, and Venezuela.
2. Department is prohibited from publishing, distributing via the Internet or other public computer based information Platform, creating derivative works (including translating), transferring, selling, leasing, licensing or otherwise making available to any unauthorized party, the Editorial Content, or a copy or portion of the Editorial Content.
3. The provision of an updated version of the Editorial Content in the FraudCapture Platform is dependent upon HMS' continuing contractual relationship with the AMA.
4. Department must ensure that anyone with authorized access to the Editorial Content will comply with these AMA End User Terms.
5. Department will accurately report to Gainwell the number of Editorial Content Users (via use of the FraudCapture Platform). "Editorial Content User" means an individual who:

   (a) accesses, uses, or manipulates Editorial Content contained in the FraudCapture Platform; or

   (b) accesses, uses, or manipulates the FraudCapture Platform to produce or enable an output (data, reports, or the like), such output could not have been created without the Editorial Content being embedded in the FraudCapture Platform; or

(c) makes use of an output of the FraudCapture Platform, and such output could not have been created without the Editorial Content being embedded in the FraudCapture Platform.

6. CPT is copyrighted by the AMA, and CPT® is a registered trademark of the AMA.
7. CPT is commercial technical data developed exclusively at private expense by the American Medical Association, 330 North Wabash Avenue, Chicago, Illinois 60611. The American Medical Association does not agree to license CPT to the Federal Government based on the license in FAR 52.227-14 (Data Rights – General) and DFARS 252.227-7015 (Technical Data – Commercial Items) or any other license provision. The American Medical Association reserves all rights to approve any license with any Federal agency.
8. The Editorial Content (provided as part of the FraudCapture Platform) is provided "as is" without any liability to the AMA, including without limitation, liability for consequential or special damages, or lost profits for sequence, accuracy, or completeness of data, or that it will meet Department's requirements. The AMA disclaims any liability for any consequences to due to use, misuse, or interpretation of information contained or not contained in the Editorial Content.
9. Department's right to use the Editorial Content terminates in the event of Department's default of these AMA End User Terms. If any of the provision of these AMA End User Terms is determined to violate any law or is unenforceable, the remainder of these AMA End User Terms will remain in full force and effect.
10. AMA is a third party beneficiary under this Supplement solely for purposes of these AMA End User Terms.

B. OPTUM SYMMETRY AGREEMENT

Certain content of the Episode Treatment Group/Procedure Quality Measurement report(s) ("**ETG/PQM Based Reports**") provided by Gainwell to Department under this Supplement are sourced from content provided under license to Gainwell by OptumInsights, Inc. ("**Optum**"). Optum requires that any client of Gainwell receiving such report(s) from Gainwell be bound by the following Optum terms and conditions:

Department shall maintain the confidentiality of the ETG/PQM Based Reports. Department shall not disclose, permit to be disclosed, or otherwise resell or transfer, with or without consideration, all or any portion of the ETG/PQM Based Reports to any third party except that Department may disclose the ETG/PQM Based Reports to its consultants, legal advisors, contractors or agents on a need to know basis ("Authorized Representatives") for the purpose of assisting, advising or rendering services to Department. Prior to the release of any ETG/PQM Based Reports to an Authorized Representative, the Authorized Representative shall execute a nondisclosure agreement which will prohibit such Authorized Representative from using such ETG/PQM Based Reports other than to assist or advise Department and from disclosing such information to any third party.

Department shall only use the ETG/PQM Based Reports for its own internal business purposes and shall not use the ETG/PQM Based Reports for any purpose outside the scope of this Supplement.

Optum disclaims all warranties of any kind relating to the ETG/PQM Based Reports, express or implied.

Optum shall not be liable to Department for any indirect, incidental, consequential, special, punitive or exemplary damages. Optum's liability to Department for direct damages relating to HMS' use of the Optum licensed software in generating the ETG/PQM Based Reports shall be limited to the amount Department has paid for use of the ETG/PQM Based Reports in the year in which the cause of action arose.

Optum shall be a third party beneficiary under this Supplement for purposes of enforcing its rights pertaining to the ETG/PQM Based Reports. Optum shall be expressly entitled to enforce its rights pursuant to the provisions of these terms as they relate to the ETG/PQM Based Reports, regardless of any alleged or actual breach or default hereunder by HMS, or any expiration or termination of this Supplement.