gainwell

Technical Proposal Attachments

Gainwell Technologies

Response to the State of Indiana

Indiana Department of Administration
Family and Social Services Administration
Office of Medicaid Policy and Planning

Premium Billing & Collection Services

Request for Proposal 22-69574

December 7, 2021

State of Indiana
Premium Billing and Collection Services
Draft Quality Assurance Plan

Contents

Introduction to Plan **2**
1 Quality Policy **3**
2 Processes and Tools for Evaluating Performance to Standards **4**
3 Performance Monitoring Staff **9**
4 Corrective Action Process **10**
5 Plan Review **11**
6 Performance Monitoring Training **12**

Introduction to Plan

Gainwell developed the quality assurance (QA) plan to continually improve and control the quality of data used to measure the performance of the premium billing and collection services contract. The QA plan describes the performance standards from the RFP that will be measured to continually evaluate the quality of service. The plan will be reviewed twice yearly with the State and be updated to reflect changes to the measurements, corrected errors, and the reporting of information.

1 Quality Policy

The Gainwell quality policy is our highest level of commitment to deliver quality services. It is the overall guiding principle for our actions and addresses the aspects of what we deliver. The quality policy holistically covers how we bring together international and customer standards relevant to our contractual and business needs.

Gainwell is committed to quality with the goal of achieving customer satisfaction by continually improving our capability to identify, develop, and provide services that are valued by FSSA and CHIP and M.E.D. Works members/payors. Our primary focus is consistency, reliability, and security while providing the responsiveness and the continuous improvement necessary to support our customers' needs.

2 Processes and Tools for Evaluating Performance to Standards

The following table lists the processes we will follow to maintain performance standards.

Table 1. Premium Billing Processes

Performance Standard	Measurement/Review Process Overview	Measuring Tool	Monitoring Frequency
Premium Billing			
a. Mail 95% of premium vouchers to new enrollees no later than twenty-four (24) hours after receiving enrollee information on the daily file.	The print reconciliation processes will be followed to verify voucher mailing. This process is detailed in the Computer Operations Procedure Manual.	Print Manager Reconciliation Window; DSIBProd – Premium Voucher Daily Summary	Daily
b. Mail 95% of premium vouchers to new enrollees no later than forty-eight (48) hours after receiving enrollee information on the monthly file.	The print reconciliation processes will be followed to verify voucher mailing. This process is detailed in the Computer Operations Procedure Manual.	Print Manager Reconciliation Window; DSIBProd Premium Voucher Daily Summary Report	Monthly
d. 99.5%of premium statements will correctly state the total amount due.	Quality analyst will compare the premium amount on the voucher to the premium amount listed in *Core*MMIS and member payment history. Please note that the premium amount listed in the Gainwell system is received from IEDSS and Gainwell has no control over the premium amount assigned to a member.	*Core*MMIS OnDemand	Monthly
Premium Collection			
a. Transfer receipt electronically to the State of Indiana daily.	Accountant maintains log to monitor time Daily Wire Transfer Request forwarded to FSSA. The log contains: time wire request forwarded to FSSA, status of CDA account (overdrawn or funded correctly), notation if FSSA contacted Gainwell regarding funding, person who completed the wire transfer request at Gainwell, and the description of why the Daily Wire Transfer Request was transferred later than 10:30 a.m.	Fifth Third Direct E-mail Wire Transfer Request Log	Daily

Performance Standard	Measurement/Review Process Overview	Measuring Tool	Monitoring Frequency
b. Notify FSSA financial management of amounts transferred daily.	Same as above	Same as above	Daily
d. One hundred percent (100%) of payments received will be correctly and timely posted.	After each check is assigned a CCN and entered into *Core*MMIS, the Daily Deposit Log, Daily Check Log, and the Cash Control Balance Report are printed. The cash control specialist signs and dates the Daily Check Log and the Cash Control Balance Report, indicating the processing and review of the cash receipts has occurred. All three cash receipt reports and all check copies along with their documentation are verified.	*Core*MMIS OnDemand	Daily
Customer Service			
a. Ninety-seven percent (95%) of all calls shall be answered within two (2) minutes.	Project manager or designee will review phone system reports daily. Real-time monitoring of incoming calls and calls in queue.	Avaya CMS Supervisor Reports and Monitoring	Daily
b. Average wait time for answered call shall not exceed forty-five (45) seconds.	Project manager or designee will review phone system reports daily.	Avaya CMS Supervisor Reports	Daily
c. The busy rate shall not exceed five percent (5%).	Project manager or designee will review phone system reports daily.	Telephone Company Reports	Daily
d. The abandoned call rate shall not exceed seven percent (7%).	The call abandoned rate can be monitored once a day.	Avaya CMS Supervisor Monitoring	Daily
e. No more than two (2) calls per payment line representative shall be in the queue at any time.	The project manager, assisted by the call center supervisor or team lead, will perform real-time monitoring of incoming calls and calls in queue.	Avaya CMS Supervisor Monitoring	Daily
f. Eighty-five percent (85%) of all issues from callers shall be resolved online.	The Project manager or designee will review CTMS reports to compare the number of opened to closed calls to make sure the percent of calls that remain open after the first contact are less than 15 percent.	CTMS	Weekly
g. Follow-up information shall be imparted to enrollees within twenty-four (24) hours from the time of first contact. If research is necessary, and the Contractor cannot ascertain the information	The project manager or designee will review CTMS reports to make sure open contacts are updated within 24 hours of the first contact. CTMS reports will also be reviewed to make	CTMS	Weekly

Performance Standard	Measurement/Review Process Overview	Measuring Tool	Monitoring Frequency
within twenty-four (24) hours, they will return the call within the twenty-four (24) hour timeline and advise when they will be able to respond with the information needed. A final written or verbal response shall be provided to ninety-seven percent (97%) of inquiries within five (5) business days, and one hundred percent (100%) within ten (10) business days.	sure other callback standards are met.		
h. One hundred percent (100%) of calls left on voice mail during or after working hours will be retrieved and returned within one (1) business day. If the Contractor is unable to reach the consumer by phone, the Contractor will mail a response within one (1) additional business day that acknowledges the request, gives the information available and, if further research is necessary, notifies the caller they will mail the appropriate information within five (5) business days. A final written or verbal response shall be provided to ninety-seven percent (97%) of inquiries within five (5) business days, and one hundred percent (100%) within ten (10) business days.	The project manager or designee will review CTMS reports to make sure VM calls are returned within 24 hours. Additionally, if a call remains open for more than 24 hours, the manager will make sure updates have been made to the caller within one business day. CTMS reports will also be reviewed to make sure additional callback standards are met.	CTMS	Weekly
Quality Assurance			
a. Review monthly five percent (5%) of incoming phones.	Each week, the project manager will listen to 5% of incoming calls. The calls will be selected randomly. The review results of each call will be documented for a variety of standards such as correctness, completeness, and politeness.	Verint	Weekly
b. Review monthly five percent (5%) of premium assignments and invoicing.	The project manager will compare the premium amount assigned to a payor in *Core*MMIS to the voucher amount billed.	*Core*MMIS	Monthly
c. Review monthly five percent (5%) of premium accounting posting.	The same process will be followed as for Premium Collection, item d.	*Core*MMIS OnDemand	Monthly

Performance Standard	Measurement/Review Process Overview	Measuring Tool	Monitoring Frequency
Reporting			
a. Submit daily financial reports no later than close of business on the following day.	Daily financial reports are posted to OnDemand; the project manager or designee will verify the reports were available each morning.	OnDemand	Daily
b. Submit status reports at least three (3) business days prior to each status meeting/conference call.	Project manager will review e-mail to make sure status reports were sent three business days prior to meetings/conference calls.	E-Mail	Monthly
c. Submit monthly program activity reports within ten (10) business days of the end of the previous month.	Project manager will maintain a master list of all reports due to the State monthly. She will make sure OnDemand reports are posted no later than the 10th business day. She will review e-mail to make sure ad hoc reports were mailed promptly.	OnDemand E-Mail PVS Master Report List	Monthly
Technical Requirements			
a. Successfully complete one hundred percent (100%) of daily and monthly file transfers.	Gainwell will continue to use our automated process that reviews all the File Exchange log files every hour. If there are any messages, an e-mail of the contents is sent to the Gainwell Production Support Team to investigate the e-mail contents and resolve any identified issues as appropriate.	File Exchange Log	Daily
b. Complete each daily and monthly file transfer with fewer than ten (10) incorrect individual records on a file. Incorrect individual records are records sent to IEDSS containing erroneous information about an individual, case, or sequence.	Gainwell will continue to use our automated process that reviews all the File Exchange log files every hour. If there are any messages, an e-mail of the contents will be sent to the Gainwell Production Support Team to investigate the e-mail contents and resolve any identified issues as appropriate. Gainwell is not responsible for inaccurate data submitted by IEDSS, but we will notify IEDSS when there are integrity issues with IEDSS transmissions.	File Exchange Log	Daily

Gainwell will use the Contract Monitoring Reporting Tool as described in its proposal to document the results of quality reviews. Each performance standard will be marked as green (met 100% of the requirement), yellow (met 90–100% of the requirement), or red (met less than 90% of the requirement). Any requirement marked as yellow or red will require a comment describing why the requirement was not met. The results of quality reviews will be submitted to the State by the 10th business day of each month for the prior month.

This section will also feature more detailed process and procedures descriptions than the draft plan submitted with the proposal and will discuss how Gainwell will meet or exceed standards.

3 Performance Monitoring Staff

Project Manager Darryl Wells is responsible for overseeing all quality monitoring. A finance team lead will assist Darryl in monitoring activities, such as account payment posting timeliness and accuracy, voucher content accuracy, monitoring daily wire transfers, verifying weekly financial balancing, refund processing, and other financial-related standards. The INXIX customer assistance team lead will assist the project manager with monitoring PVS call center staff members and other customer service monitoring activities, as needed. The INXIX print operations supervisor will monitor the accuracy and timeliness of the voucher printing and mailing. The production support team will monitor file transfers.

4 Corrective Action Process

If Gainwell identifies a recurring quality problem, we will create and submit a corrective action plan (CAP) to FSSA. The CAP will follow a standardized format. Gainwell will meet with FSSA to determine the threshold criteria of a quality event that will trigger a CAP. The following table shows the format of the CAP.

Table 2. Corrective Action Plan Format

Plan Element	Description
Problem Statement	Description of the quality problem
Root Cause	Description of what is the root cause of the problem (system, training, process, etc.)
Corrective Actions	Description of the specific actions needed to permanently fix the problem and prevent recurrence
Person(s) Responsible	Name of persons responsible for executing the corrective actions
Due Date	Date(s) the correction actions are to be completed

We will review CAPs no later than 6 months after implementation to help make sure the problem has not recurred.

5 Plan Review

Gainwell will review the QA plan with FSSA on delivery of the final draft, which is due 60 days after contract signing. Gainwell will fully cooperate with FSSA on all plan quality reviews, including providing access to all case records and information. Gainwell recommends the QA plan be reviewed every six months with FSSA after the initial review.

6 Performance Monitoring Training

On delivering and reviewing the QA plan with FSSA, the Project Manager Darryl Wells will schedule a training session on the techniques used to monitor Gainwell's performance to contract standards. The Gainwell and FSSA staff who support the contract will receive this training.

Following is our proposed agenda for performance monitoring training:

- Overview of Continuous Improvement Policy for premium billing and collections
- Performance Metrics Review
  - Review Section 1 of this plan for a complete list of performance metrics
- Review roles and responsibilities
- Review PWB Data Entry Portal
  - How to access the portal
  - How to add requirements
  - How to update requirements
  - How to search for requirements
- Review InSight Dashboard reporting tool
  - How to access the reporting tool
  - Policy for using the reporting tool
  - How to generate a monthly report
  - How to update, save, and export the monthly report
- Review Verint recording system
  - How to access the system
  - How to listen to real-time and recorded calls

State of Indiana
Premium Billing and Collection Services
Proposed Site Security Plan

Contents

1 Introduction to Plan 3
2 HIPAA Considerations 4
2.1 Monitoring and Oversight Activities 4
2.2 Security and Protection of Systems, Procedures, Practices, and Facilities 5
3 Data Security 7
3.1 Secure Controlled Area for Storage 7
3.2 Secure Email 7
3.3 Desktop and Laptop Encryption 7
3.4 Password Protection and Reset Capability 8
3.5 Additional Data Security Considerations 8
3.5.1 Control and Accounting of Data 9
3.5.2 Confidentiality of Passwords and IDs 9
3.5.3 Access for Gainwell Staff Members 10
3.5.4 Quarterly Workstation and Facility Audits 10
3.6 Traffic and Network Monitoring Software and Tools 10
3.6.1 Detect and Prevent Unauthorized Use of Resources 10
3.6.2 Prevent Adware or Spyware from Deteriorating System Performance 11
3.6.3 Perform Daily Virus Blocking Software Updates 11
3.6.4 Monitor Bandwidth Usage 11

1 Introduction to Plan

The Family and Social Services Administration (FSSA) requires a secure solution that protects data from anticipated threats or hazards and restricts its availability to appropriate staff members and other designated individuals and organizations using a standardized approach to physical security besides secure system applications and data security capabilities. Gainwell will maintain compliance with the Health Insurance Portability and Accountability Act (HIPAA) regulations and adjust our operations to help support compliance with updates made to HIPAA requirements. To meet FSSA's requirements for physical security, we need to provide a comprehensive approach that also addresses maintaining the confidentiality of the data we work with. We will accomplish this by applying Gainwell's fundamental values to our team's personal diligence in working with sensitive Indiana information every day.

As the premier provider of Medicaid Management Information System (MMIS) solutions, Gainwell also recognizes the additional responsibility for managing confidential protected health information (PHI), financial data, and FSSA's own data.

The Gainwell HIPAA Security Policy states the following:

> "To be compliant to the HIPAA regulations, both security and privacy solutions must be considered. Gainwell shall implement standards in accordance with the Security rule to ensure: Confidentiality, integrity, and availability of electronic health information with effective administrative, physical, and technical safeguards."

The policy continues with the statement that Gainwell will implement "… security solutions to address the organization's infrastructure requirements to ensure secure and private communication and storage of confidential electronic PHI."

*Core*MMIS already includes the security structure needed to meet security compliance standards because of the joint efforts of FSSA and Gainwell Privacy and Security Management team during HIPAA remediation activities. Gainwell has demonstrated and will continue to demonstrate our commitment to reinforce enterprisewide system security. Gainwell will continue to work with FSSA to meet security requirements as they relate to this contract.

Gainwell developed a comprehensive system security process for *Core*MMIS by using the National Institute of Standards and Technology (NIST) and the Gainwell Enterprise Security Policies and Standards (ESPS) framework as guides. Developed by the Gainwell Security and Privacy Office that provides guidance and direction to help secure the Gainwell environment, ESPS combines security best practices and expertise from around the globe to deliver the policies, requirements, control standards, and implementation procedures necessary for a complete security solution.

2 HIPAA Considerations

To enhance HIPAA security compliance, Gainwell has integrated HIPAA security rule standards into our own. This integration is accomplished with the Enterprise Security Information System (ESIS). ESIS is an automated Web-based tool that maintains corporate policies, requirements, and control standards. Each HIPAA standard has been mapped to relevant Gainwell corporate policies and applicable requirements and control standards. The HIPAA ESIS tool provides the framework for establishing procedures that support existing Gainwell policies and other relevant federal and state security requirements.

The HIPAA privacy and security rules and NIST publications serve as our guides and helped frame our current approach to meeting security and confidentiality requirements. The following sections describe our current approach to meeting security and confidentiality requirements under the Indiana Health Coverage Programs (IHCP) fiscal agent contract. Additionally, we will apply this proven approach to secure and maintain confidentiality of data associated with this contract:

- Monitoring and Oversight Activities
- Security and Protection of Systems, Procedures, Practices, and Facilities
- Data Security

2.1 Monitoring and Oversight Activities

Gainwell has taken a proactive approach to managing the HIPAA privacy and security rules for the IHCP. We have created a comprehensive Monitoring and Oversight Plan that will be used by FSSA and Gainwell to help support the security and confidentiality of PHI.

HIPAA compliance is of the utmost importance to Gainwell. Periodic risk assessments are performed to determine gaps that may exist based on changes to the environment. Risks are identified for project activities. However, periodic risk assessments are needed to make sure security requirements are addressed appropriately. Project plans are then developed to address identified gaps and include ongoing monitoring and oversight activities. The leadership staff will be responsible for conducting periodic risk assessments.

Our goal is to continually strengthen the privacy and security policies and procedures to minimize the risk of PHI exposure. Monitoring and oversight activities that our leadership will perform include the following:

- Quarterly workstation and facility audits are performed to verify that privacy and security policies are being followed.
- Facility badge access is reviewed monthly and new personal identification numbers (PINs) are assigned semiannually to reduce the risk of unauthorized entry.
- Security awareness reminders are sent out to Gainwell users to remind them of the important role they play in securing PHI. Topics such as laptop security, use of certified mail, the definition of PHI, password security standards, use of external media, the definition of a security incident, how to report an incident, and information-handling guidelines are sent to each employee to communicate the proper security practices to follow.
- Quarterly *Core*MMIS Access Audit reports provided from the fiscal agent team to the leadership team will be reviewed and updated by leaders to verify that appropriate access to PHI is monitored and the appropriate people have access to the data based on their roles.

- Internal security evaluation is performed to determine if privacy and security procedures are being followed appropriately. Results of the evaluation are used to determine if additional employee training is needed to address specific privacy and security policies and procedures.
- Laptop and desktop audits are performed to detect and remove unauthorized software or PHI data as equipment is refreshed.
- Business continuity and disaster recovery plans are reviewed and updated annually.
- Privacy and security incidents are identified, documented, logged, and reviewed with FSSA.
- Privacy and security training is required for employees and contractors before access is granted to applications containing PHI.
- Network security is reviewed, monitored, and secured to verify that only approved traffic is allowed into the network.
- Participation in Gainwell's Information Protection Week continues to heighten privacy and security awareness of Gainwell staff members. Posters are displayed on each floor, security awareness bulletins are sent out by email, presentations are delivered in team meetings, and a security quiz is made available for employees.

We continually look for ways to improve our privacy and security practices. In recent years, the increased visibility of the number of lost or stolen mobile media devices—such as laptops and other mobile storage media—has caused private-sector and government entities to mitigate the possibilities of being affected by this trend. Gainwell has taken our responsibility to protect customer and consumer data seriously by investigating various alternatives to develop solutions and take additional measures such as requiring encryption of data on laptops and desktops to mitigate the potential risk of lost or stolen PHI data.

Gainwell has established a Privacy and Security Work Group that comprises members of each Medicaid state to share and brainstorm ideas to improve monitoring and compliance. A regional steering committee also has been established to lead this work group to develop common standards, best practices, and methodologies.

The State of Indiana has benefited from Gainwell's participation in the Privacy and Security Work Group and steering committee. Information shared during these meetings is routinely communicated during the privacy and security meetings between Gainwell and FSSA. The Gainwell privacy and security coordinators have used this information to strengthen policies and procedures used in daily operations. Our privacy and security coordinators routinely evaluate and revise policies and procedures as needed to help promote the security of IHCP data. This ongoing evaluation minimizes the risk of loss, modification, or disclosure of PHI. This knowledge and experience will be applied to this contract, and the leadership team will be responsible for implementing Gainwell's HIPAA privacy and security standards, best practices, and methodologies and monitoring compliance against these to help make sure data is protected.

2.2 Security and Protection of Systems, Procedures, Practices, and Facilities

Gainwell verifies that systems, procedures, practices, and facilities are secure and protected through the many audits, evaluations, and methodologies mentioned previously. We provide a solution that is constructed so that each aspect of security—from data to physical security—is

addressed. Using the ESPS framework described previously, Gainwell has developed comprehensive system security procedures. ESPS combines security best practices and expertise from around the globe to deliver the policies, requirements, control standards, and implementation procedures necessary for a complete security solution.

Gainwell is housed in secure, self-contained areas on three floors of the building at 950 North Meridian Street and a secure workspace at 450 E. 96th Street (Parkwood). Physical access is limited to authorized workforce members. Authorized Gainwell workforce members enter secure doors by using a badge reader, which requires a four-digit access code for entrance. Each Gainwell workforce member has a unique access code that permits entrance into the facility. The four-digit access code is updated on a semiannual basis and is auto-assigned by the badge system. The privacy officer ensures that the Badge Reader Access Report is compared to the organizational chart monthly to identify discrepancies. If discrepancies are noted, they are documented and corrected immediately. Additionally, on a quarterly basis, leaders review the Badge Reader Access Report to ensure that the Gainwell workforce has access only to appropriate areas.

All Gainwell workforce members are responsible for assisting in controlling and validating a person's access to facilities. In other words, workforce members should question unfamiliar individuals and report their presence to the Gainwell security officer, as needed.

Identified FSSA personnel are authorized access via the badge reader system and are issued security badges in accordance with their level of assigned access. Personnel are screened quarterly in accordance with the procedure outlined previously and verified with the facility coordinator.

Access by authorized contracted vendors is provided within a defined location that has appropriate computer workstations. Vendors must sign in and out using the Vendor Log.

Visitors must be approved for entrance at the reception desk, sign a visitation log, and be always escorted by an authorized Gainwell workforce member.

The privacy and security officers meet with the landlord and building security staff to review policies and procedures for physical access to the Gainwell facility, as well as expectations that security and janitorial staff will follow Gainwell procedures (along with their own security control standards). These expectations include how to secure badges and access keys, including turnover procedures for change of staff between shifts. This review occurs at a minimum annually and is included on the Privacy and Security Work Plan to track compliance with this requirement.

3 Data Security

FSSA can be confident in the data security and protection of Children's Health Insurance Program (CHIP) and Medicaid for Employees with Disabilities (M.E.D. Works) data. Users are granted or denied access according to their user profiles. Profiles are determined jointly between FSSA and Gainwell staff members. In the following subsections, we describe our approach to data security:

- Secure Controlled Area for Storage
- Secure Email
- Desktop and Laptop Encryption
- Password Protection and Reset Capability
- Additional Data Security Considerations
- Traffic and Network Monitoring Software and Tools

3.1 Secure Controlled Area for Storage

Gainwell provides secure storage for electronic, hard-copy, and backup data information within the facility and off site. Offsite storage facilities are located near our Indianapolis facility. Records are maintained based on the record retention schedule as published by the Indiana Commission on Public Records.

3.2 Secure Email

Gainwell and FSSA use DataMotion for encrypting email containing PHI or other confidential information. The DataMotion licenses are provided to help facilitate confidential email communication between FSSA and Gainwell staff members. Gainwell proposes the continued use of the DataMotion solution because encryption provides secure transmission of confidential information, which in turn protects member PHI. The Gainwell Privacy and Security team worked with FSSA to evaluate and select the existing email encryption software package that met the requirements of the HIPAA privacy and security rules and Indiana Family and Social Services Administration (FSSA) requirements.

3.3 Desktop and Laptop Encryption

The Gainwell Security team coordinated efforts with FSSA to evaluate and select a laptop encryption software tool that would reduce the risk of PHI being compromised. Gainwell took additional steps to minimize this risk by implementing policies and procedures, such as the following:

- Provide best practice guidelines for employees to follow when removing laptops and PHI from the Gainwell facility
- Educate employees not to save PHI data on workstations
- Perform laptop and desktop audits to look for unauthorized software and PHI

Gainwell has installed an additional software encryption solution on desktops within the facility, called Pointsec. Desktops and laptops will be encrypted to continue our ongoing efforts to secure the environment and mitigate risk of exposure.

3.4 Password Protection and Reset Capability

Gainwell provides password protection and password reset capability for user authentication and authorization to our systems. Additionally, the *Core*MMIS system prohibits generic or shared passwords. Applications require a unique user ID and a password that expires at least every 30 days. This password also can be changed at the user's discretion and must follow the criteria of a strong password. Incorrect user ID and password combinations will result in an error to the user attempting to log on. After three unsuccessful logon attempts, the user ID will be disabled.

An automated password reset function in *Core*MMIS allows the password to be reset by answering questions and requires no intervention from security personnel. Inactivity for 30 days or longer will result in a suspended user ID and can only be reset by security personnel.

3.5 Additional Data Security Considerations

Security for *Core*MMIS is built on a fundamental philosophy—provide the right information to the right authorized user and only to the right authorized user.

The *Core*MMIS security repository maintains security and user permissions. The security administration module allows for the efficient creation and maintenance of security. The user security categorizes access into different security levels defined by FSSA. The categories include users, groups, and roles. Through these security levels, *Core*MMIS provides the permission settings necessary to perform required business functions.

User security within *Core*MMIS is based on user ID, user group, and business role. Additionally, database profiles are used to control *Core*MMIS program access to the Oracle database. Security protection is extended at the application level (screen access) and the system level (file access). Security controls within the Enterprise Security Architecture and *Core*MMIS require that users have a unique user ID and password combination. Inherent features of *Core*MMIS that provide additional levels of security are as follows:

- Password complexity requirements
- Lockouts for multiple incorrect authentication attempts
- Regular, frequent, and configurable mandatory password changes

User- and role-based security is assigned for specific applications and data, including access restrictions to protected and confidential information, in accordance with HIPAA privacy and security requirements. User- and role-based security is assigned according to HIPAA-compliant minimum necessary standards. Each user has a unique logon ID to access the system.

Gainwell management is required to approve access for Gainwell staff based on roles and responsibilities. Gainwell personnel and contract staff are required to successfully complete privacy and security training before receiving a logon ID and password. The individual user will be allowed to access applications on the system only after entry of a password with the correct user ID. At regular and configurable intervals, passwords for users will expire and users will be prompted to create new passwords. The default expiration period is 30 days.

In the following subsections, we describe our approach to additional data security considerations:

- Control and Accounting of Data
- Confidentiality of Passwords and IDs
- Access for Gainwell Staff Members
- Quarterly Workstation and Facility Audits

3.5.1 Control and Accounting of Data

Gainwell will strictly adhere to the data security requirements identified in this RFS. We provide complete control and accounting of the data received, stored, used, or transmitted. A new vendor may not fully understand the complexity of the system, data interfaces, or the overall environment to control or account for data. Gainwell has demonstrated our ability to provide proven administrative, physical, and technical security of FSSA data as the Indiana Medicaid fiscal agent, and we will apply our knowledge and experience to this contract.

The integrity and confidentiality of the data is protected by safeguards that verify information is not released without proper consent. Individuals with access to confidential data will agree to abide by State confidentiality rules and policies. To help make sure users understand their responsibility for maintaining confidentiality of the data in *Core*MMIS, the user confidentiality agreement was introduced. Users are required to read and accept the terms and conditions of this agreement electronically through the application. New users are required to read and accept the terms and conditions of the confidentiality agreement before gaining access to *Core*MMIS and are prompted to review and accept it annually. The annual renewal process serves as a reminder of the user's responsibility to protect the system data. Additionally, this will help to verify accountability of the user's actions if the data is misused or compromised.

Gainwell takes the matter of potential or actual misuse of data seriously. Protecting customer data is a primary objective of our existing solution, as exemplified through our enterprise security, application security, physical security, audit trails, and reporting. We designed our privacy and security processes and procedures to protect data from misuse or accidental disclosure.

For example, user updates and changes to *Core*MMIS data are strictly controlled, and appropriate audit trails are maintained. These audit trails contain the unique logon ID (or batch update identifier), date, and time of the change. Each record changed is updated with the date of the change and the identification of the person making the change.

This combination of online security and data access protects important information while increasing productivity as users find information easier to retrieve and use. Based on security profiles, users are limited not only to the windows they are authorized to access, but also to the data content.

3.5.2 Confidentiality of Passwords and IDs

Gainwell provides confidentiality of usernames and passwords. Suspicious activity and violations are reported to the Gainwell Privacy and Security staff for investigation. Individuals are required to use unique user IDs and passwords. Violations of this requirement are reported as security incidents.

A key component of this approach will be continuous, effective training on the proper use of the system and data security. Gainwell employees are required to attend security training that highlights the importance of confidential user IDs and passwords.

3.5.3 Access for Gainwell Staff Members

After Gainwell staff members have successfully completed the required privacy and security training, they are provided access to the system based on their roles in the organization. Management creates a Security Request Form and submits it to the security administrator to initiate system access. Gainwell will use the Web security request to request, change, or delete system security access for staff members.

3.5.4 Quarterly Workstation and Facility Audits

Gainwell performs a periodic physical privacy and security audit to continue to reinforce the importance of protecting PHI. Our management team performs social engineering and walkthroughs of the facility, looking for violations to the published Gainwell privacy and security policies and procedures. Results are reviewed to help facilitate compliance to the privacy and security policies and procedures. Based on the audit findings, corrective action plans (CAPs) are discussed and improvements monitored. Routine auditing of physical security capabilities will assist in the protection of physical documents and electronic data and assets.

3.6 Traffic and Network Monitoring Software and Tools

We discuss our approach for providing traffic and network monitoring software and tools in the following subsections:

- Detect and Prevent Unauthorized Use of Resources
- Prevent Adware or Spyware from Deteriorating System Performance
- Perform Daily Virus Blocking Software Updates
- Monitor Bandwidth Usage

3.6.1 Detect and Prevent Unauthorized Use of Resources

Gainwell best practices dictate a multilevel approach to securing the data and assets under our control. Besides the user authentication and authorization process described previously, a suite of technologies is employed at different levels of the infrastructure for an added layer of protection against unauthorized access.

High-speed firewalls and devices with IPS capabilities are situated on every entry point into the Gainwell network. The firewall policies governing the type of traffic that passes between the networks limit access to the systems and services that are required for communication between the devices and the user. IPS devices continually monitor the traffic for suspicious activity as it traverses the network. These devices are configured to call our email system personnel depending on the level of severity the threat poses.

Management control of these devices is critical in maintaining a secure environment. A breach in security of any of these devices would allow access to the configuration files, which govern the use and control of the network. Therefore, the management consoles are situated on a secure segment of the network. To fortify the protection of these devices, the Telnet protocol is not an approved method for system support access for configuration changes. Secure shell

(SSH) is mandatory for accessing network management devices, creating a secure method to transport administrator user ID and password information. Change control software monitors configuration changes and can alert system personnel when changes to the configuration are made. Additionally, this software has a rollback feature that will revert to a previous configuration version.

Gainwell is one of the industry leaders in security, and we bring this security awareness and action to FSSA in operational support areas.

3.6.2 Prevent Adware or Spyware from Deteriorating System Performance

Gainwell has installed software programs that scan our network and PCs for adware and spyware threats and removes them immediately. Adware and spyware can reduce network performance and expose confidential data to unauthorized users. By eliminating adware and spyware threats, sensitive data remains secure.

3.6.3 Perform Daily Virus Blocking Software Updates

Virus blocking is an Gainwell priority, and we work with McAfee, a leader in antivirus technology. Gainwell will protect machines and networks with McAfee software. Scheduled scans and real-time memory monitoring will further prevent the spread of threats introduced into the Gainwell infrastructure.

The antivirus software looks for updated virus signature files every day. These files contain information on how the software can detect new viruses. The antivirus software contains two methods of virus detection: real-time monitoring and hard-drive scanning.

Real-time monitoring provides multiple features. It scans for viruses in computer memory and hard-drive files as actions are performed on them. These actions include opening Word documents, launching applications, and copying files to and from a network. Real-time monitoring scans files moving to and from computers and networks.

Hard-drive scanning examines files on the user’s hard drive for virus infections. This approach differs from real-time monitoring because real-time monitoring scans only files that are opened or copied, whereas hard-drive scanning will scan all files on the hard drive.

3.6.4 Monitor Bandwidth Usage

Gainwell monitors current system performance by examining many of its components, including bandwidth usage and possible bottlenecks. Packages such as Solarwinds Network Performance Management (NPM) and Multi Router Traffic Grapher (MRTG) enable us to monitor network devices including local area network (LAN) and wide area network (WAN) connections, create baselines, facilitate performance and response time analysis, simulate traffic through the traffic generator utility, and analyze a problem from network to application.

Project Manager

Darryl Wells

Experience Summary

Darryl has more than 20 years of business operations and information technology management experience in Medicaid and Billing and Accounts Receivable. Primary responsibilities include managing business and technical teams including provider field agents, provider enrollment staff, software developers, business analysts, and project managers. Special areas of emphasis during the past several years include staffing, onboarding, and training project managers and administering their benefit, performance management, career development, and compensation. Darryl's skills and experiences allow him to effectively adapt to new roles and responsibilities assigned based on the priorities of the organization.

Relevant Expertise

Domain	Years
Billing and Receivables	08
Business Requirements and Analysis	10
Claims Processing	05
Disaster Recovery	03
Drug Rebate	02
Process Development	10
Project Management Office	05
Provider Enrollment	02
Provider Management	02
Resource Management	10
Reference	02
MAR/MSIS	02
SDLC	20

Experience

Corporate Project Management Capability
Human Resources Manager, Gainwell Technologies
July 2019 - Present

Responsible for staffing, hiring, and onboarding project management professional positions for the Ohio, Indiana, Kansas, and Wisconsin Medicaid accounts. Includes HR activities such as training, development, performance management, and salary administration for 45 employees.

Indiana Medicaid
Service Now Implementation Manager, DXC Technology
June 2019 – March 2020

Responsible for managing the requirements, design, and schedule for Service Now application replacement of Service Manager. Included gap analysis of Indiana's local Service Manager application compared to the DXC Technology corporate Service Now solution, which was based

on Ohio Medicaid's Service Now solution. Supervised the local business analyst and developer resources and managed the relationship with the corporate Service Now team.

Indiana Medicaid
Disaster Recovery Coordinator, Gainwell Technologies
March 2018 -- Present

Responsible for managing the local resources supporting the annual Indiana Medicaid disaster recovery exercise. This exercise replicates the production Indiana Medicaid system in Orlando, FL to Colorado Springs, CO, and verifies that data and functionality is present and operational.

Indiana Medicaid
Optum FSSA EDW Liaison, Gainwell Technologies
March 2017 – Present

Responsible for identifying and discussing Core MMIS modifications that impact the State's Enterprise Data Warehouse. Includes educating the EDW vendor Optum, and addressing their comments and feedback regarding CoreMMIS database tables. A weekly meeting is conducted to review action items, inquiries, defects, and development projects that may impact Optum's EDW processing. Vendor testing is coordinated between Gainwell Technologies, Optum, and FSSA.

Indiana Medicaid
Core MMIS Transition Manager, DXC Technology
January 2015 – February 2017

Responsible for identifying, addressing, and acclimating Medicaid users to the differences between the existing Indiana*AIM* Medicaid solution and the Indiana Core MMIS Medicaid solution. All stakeholders were contacted, review sessions were held, clarifications were made, and materials distributed, to minimize disruption in operations.

Indiana Medicaid
PMO Business Analyst Manager, Gainwell Technologies
February 2011 – Present

Responsible for managing a team of business analysts who generated the requirements and business design documents to support IndianaAIM and CoreMMIS PMO project development. Included staffing, onboarding, training, and development of team members on the change management process published by the PMO.

Indiana Medicaid
Provider Enrollment Supervisor, Hewlett Packard
August 2009 – January 2011

Responsible for managing the provider enrollment team in the inspection of provider enrollment applications, verification of licensure, and finalizing enrollments based on contract standards. Implemented inventory management reporting tools, with a focus on consistency across team members to improve overall accuracy and timeliness.

Indiana Medicaid
Systems Manager, EDS an HP Company
December 2006 – July 2009

Responsible for managing the day-to-day work of more than 20 developers. Included working with project managers to manage and allocate resources to projects based on priority, as well as integrating their systems maintenance responsibilities and production support duties.

Indiana Medicaid
Business Support Manager, EDS an HP Company
May 2005 – November 2006

Responsible for managing a team newly formed and responsible for systems documentation, reference management, and Medicaid Statistic Information Systems (MSIS). Included generating and improving the quality of available documentation and managing changes to claims reference processing tables.

Indiana Medicaid
Client Services Director, EDS an HP Company
October 2003 – April 2005

Responsible for the provider services operational area, which included the field agents, provider enrollment, and the call center. Included attending provider association meetings and coordinating the annual provider seminar.

Technical Support Center
NVBARS Manager, Electronic Data Systems
September 1995 – September 2003

Responsible for leading a team of project managers responsible for General Motors' Non-Vehicle Billing and Accounts Receivables application. Included management functions such as staffing, onboarding, training, career development, and performance management.

Training/Education

Degree/Certificate	Institution
Bachelor of Science, Computer Science & Business	Butler University, Indianapolis, IN
EDS Software Engineering Development Program	Electronic Data Systems

Professional Certifications or Affiliations

- Project Management Institute, Project Management Professional
- Information Technology Infrastructure Library Certified (ITIL)
- Software Engineering Institute Capability Maturity Model (SEI-CMM)

Premium Vendor Services Complaint Tracking Log

Date Notified	CTMS Tracking Number	Name	Payer RID	Reason	Incident Date	Referred To	Research/Actions	Completion Date	Project Manager QC Date

Gainwell Technologies LLC - State of Indiana
950 N. Meridian St
Indianapolis, IN 46204

State of Indiana
Premium Billing and Collection Services
Draft Transition Plan

Contents

1 Gainwell's Approach to Transition 2
1.1 Planning 2
1.2 General Planning with State 3
1.3 General Planning with Successor 3
1.4 Develop Transition Plan 4
1.5 Pre-Turnover of Data 4
1.5.1 Nine-Month Requirement 4
1.5.2 Six-Month Requirement 4
1.6 Transition Management 4
1.7 Transition Services 5
1.7.1 Cooperation with Successor 5
1.7.2 Turnover of Archived Materials 5
1.8 Resolution of Transition Issues 6
2 Contract Closeout Services 8
3 Financial Reconciliation 9
4 Post-Transition Reporting 10
5 Appendix: Transition Manager Qualifications 11

1 Gainwell's Approach to Transition

Part of Gainwell's commitment to serving Indiana is to conduct a smooth transition to a successor fiscal agent (FA) at the end of the contract. We want the transition to be as imperceptible as possible for the State and its program members.

The Transition phase represents a period of transition during which premium billing and collection services and related operation and technical support activities are turned over to Family and Social Services Administration (FSSA) or a subsequent vendor. The completion of the Transition phase, which is a final step in Gainwell's customer service and project management approach at contract end, is crucial. During the Transition phase, we will take action necessary to support a turnover that minimizes disruption to premium billing and collection services.

Specifically, we have the following objectives for the Transition phase:

- Support an orderly, controlled transition to FSSA or a designated vendor by fully defining roles and responsibilities
- Help prevent service disruptions for members
- Help support continuing processing and smooth operations for FSSA
- Meet obligations through the last day of contractual responsibility
- Maintain positive relationships with FSSA, the member community, and associated State agencies

Our transition approach for Indiana is based on past successful transition plans. The detailed systems documentation and user manuals, along with the automated nature of premium billing and collection services, support an efficient transition process.

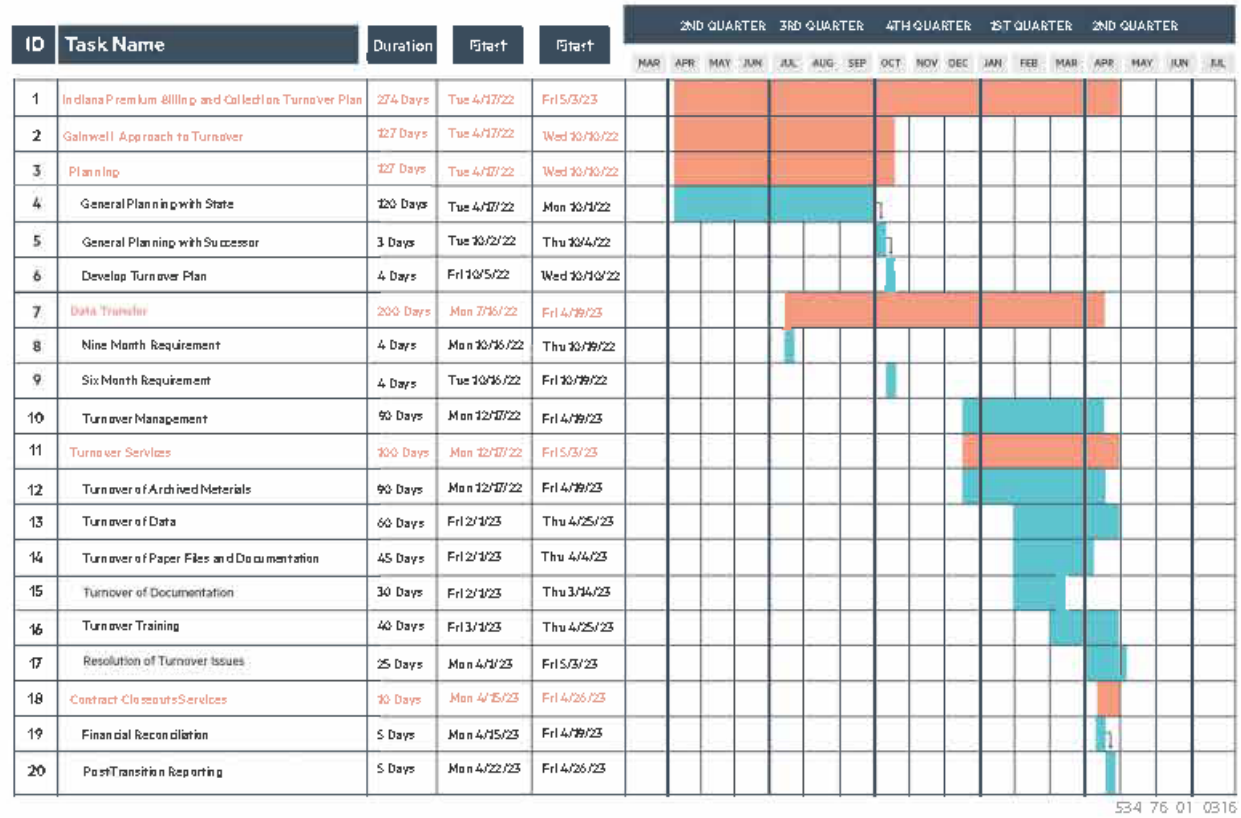
1.1 Planning

Gainwell will create a schedule for transition activities and submit the schedule for FSSA's approval. Members of our premium billing and collections team, using proven project management tools and standards, will perform transition tasks to meet the State's objectives. With these tools, including Microsoft Project, SharePoint, and real-time reports and data updates from premium billing and collection services, we can perform these tasks efficiently and effectively to help FSSA meet its transition objectives.

Gainwell will support an orderly, controlled turnover of contract operations by defining and communicating our activities, roles, and responsibilities. We will assist FSSA in minimizing service disruption to the member communities.

An example of key activities in a transition work plan is depicted in the following figure.

Figure 1. Sample Transition Work Plan Activities



ID	Task Name	Duration	Start	Finish
1	Indiana Premium Billing and Collection Turnover Plan	274 Days	Tue 4/17/22	Fri 5/3/23
2	Gainwell Approach to Turnover	127 Days	Tue 4/17/22	Wed 10/19/22
3	Planning	127 Days	Tue 4/17/22	Wed 10/19/22
4	General Planning with State	120 Days	Tue 4/17/22	Mon 10/3/22
5	General Planning with Successor	3 Days	Tue 10/2/22	Thu 10/4/22
6	Develop Turnover Plan	4 Days	Fri 10/5/22	Wed 10/19/22
7	Data Transfer	200 Days	Mon 7/18/22	Fri 4/28/23
8	Nine Month Requirement	4 Days	Mon 10/16/22	Thu 10/19/22
9	Six Month Requirement	4 Days	Tue 10/16/22	Fri 10/19/22
10	Turnover Management	90 Days	Mon 12/19/22	Fri 4/28/23
11	Turnover Services	100 Days	Mon 12/19/22	Fri 5/3/23
12	Turnover of Archived Materials	90 Days	Mon 12/19/22	Fri 4/28/23
13	Turnover of Data	60 Days	Fri 2/3/23	Thu 4/25/23
14	Turnover of Paper Files and Documentation	45 Days	Fri 2/3/23	Thu 4/4/23
15	Turnover of Documentation	30 Days	Fri 2/3/23	Thu 3/14/23
16	Turnover Training	40 Days	Fri 3/3/23	Thu 4/25/23
17	Resolution of Turnover Issues	25 Days	Mon 4/3/23	Fri 5/3/23
18	Contract Closeouts Services	10 Days	Mon 4/17/23	Fri 4/28/23
19	Financial Reconciliation	5 Days	Mon 4/17/23	Fri 4/28/23
20	Post Transition Reporting	5 Days	Mon 4/22/23	Fri 4/28/23

1.2 General Planning with State

We are committed to meeting the transition requirements detailed in the Request for Proposal (RFP) for a complete, uninterrupted, and successful transition. We will track State, Gainwell, and the replacement vendor responsibilities associated with the transition in the Microsoft Project work plan.

We will confirm work requirements, gain the participation of those best qualified to do the work, and develop the appropriate schedule. We will conduct recurring project status meetings with FSSA to discuss transition activities, status of deliverables, tasks, milestones, resources, project risks, action items, progress, and issues.

We will maintain sufficient staff to continue to support the performance levels provided throughout the operations phases. We will include built-in staff reductions as components of the program operations that are turned over to a subsequent vendor. We will work closely with FSSA to schedule the timing of any transition of incumbent staff to a subsequent vendor.

1.3 General Planning with Successor

We will work closely with FSSA and the successor during the planning for the Transition phase to provide uninterrupted service to the member communities. We recognize that during a transition, FSSA would require our full cooperation and assistance to achieve a smooth transition of system operations to the State or its designated vendor. Our schedule of activities will prioritize, sequence, and time the transition tasks, providing a basis of communication and

activities among FSSA, Gainwell, subcontractors, and the successor, minimizing disruption during the Transition phase. The transition manager will collaborate with FSSA, the subcontractors, and the successor to direct the development of the activity.

1.4 Develop Transition Plan

In preparing the Transition Plan, Gainwell will incorporate proven project management techniques, diverse transition experience, a comprehensive understanding of FSSA's transition requirements, and a commitment to the continued smooth operation of premium billing and collection services.

1.5 Pre-Turnover of Data

1.5.1 Nine-Month Requirement

Nine months before the contract expiration date, or any extension thereof, Gainwell will transfer the following information, on a medium specified by the State, to the director of Medicaid or designee:

- A copy of nonproprietary systems or database(s) used, including a copy of the data, data model, and data dictionary
- Internal logs and balancing procedures used during the contract to maintain compliance with operational requirements
- Other documentation including, but not limited to, user, provider, and operations manuals and documentation of interfaces developed to support business activities between contractors

1.5.2 Six-Month Requirement

Six months before the contract expiration date or any extension thereof, Gainwell will begin training State personnel, or its designated agent's staff, in the operations and procedures performed by Gainwell premium billing and collections staff. Such training will be completed at least 2 months before the contract expiration date or any extension thereof. Such training includes, but is not limited to, the following:

- Data entry processing
- Computer operations
- Controls and balancing procedures
- Other manual procedures

1.6 Transition Management

The Gainwell transition manager, using proven project management principles, will work with FSSA, subcontractors, and the successor during the Transition phase to develop a detailed work plan using Microsoft Project. The transition manager will have at least 1 year of premium vendor experience. The work plan will track deliverables, tasks, milestones, and resources. We will organize it as requested by FSSA to facilitate requirements traceability and to simplify State resource availability. This plan will enable us to effectively communicate the status of premium

billing and collection services. We will schedule walkthroughs of the plan and make agreed-on updates, as required.

Our experience has taught us about the activities, time, effort, and risks associated with the transition of a premium vendor program. FSSA will benefit from our experience as we develop a solid plan for turning over premium billing and collection services business operations to another vendor. The plan will clearly identify the transition tasks and activities, scheduled start and completion dates, status, the assigned resource, and responsible vendor.

To develop the transition schedule, the Gainwell transition manager will work closely with FSSA to define and align transition activities and milestones by creating a work breakdown structure (WBS) and network diagram. We will determine start and finish dates for project activities based on FSSA's priorities and estimate the duration of each activity from our experience with past MMIS transitions of this size. We will create a detailed schedule in Microsoft Project based on the unique requirements of premium billing and collection services.

Gainwell will provide a timeline for each transition item within each business area, based on FSSA's needs and the incoming vendor's transition plan. For each business area, a logical start and completion date will be set, given its priority in the transition, interdependencies, and resource constraints.

1.7 Transition Services

Gainwell wants to make sure FSSA is confident about the aspects of the transition. The cooperation of the current contractor is vital to a smooth turnover and transition of premium billing and collection services. Our corporate presence in Indiana attests to our commitment to preserving our relationship, and we will fulfill our transition obligations responsibly.

1.7.1 Cooperation with Successor

We will cooperate with the successor, providing required transition services, including meeting with the successor and creating work schedules agreeable to FSSA, Gainwell, and the successor.

The Gainwell transition manager will continue to provide support beyond contract termination to fulfill the role of post-transition manager and work with the new vendor following contract termination. This individual will have in-depth knowledge of the transition activities, approach, and status and will be prepared to begin post-transition support immediately. The manager will provide FSSA and the subsequent vendor with support for post-transition activities.

FSSA will receive a Transition Result Report that contains the final status and results of each task identified in Gainwell's transition plan.

1.7.2 Turnover of Archived Materials

The turnover of premium billing and collection services data and documentation will be included as tasks in the transition schedule. For each functional area, we will identify files, paper and manual documents, processes, and procedures that must be maintained to provide continuous operations.

Archived records will remain archived. They will be turned over to FSSA's designee at the agreed transition date. Records that are not archived will be included in the transition inventory if required to support continued delivery of services to eligible members, as agreed on with

FSSA. Gainwell will make these records available for pickup by FSSA or its designee during the Transition phase. Financial records will be retained and made available to FSSA in accordance with the contract, as necessary, to assist in confirming that Gainwell has properly fulfilled its undertakings according to the terms of the contract.

1.7.2.1 Turnover of Data

Gainwell will provide FSSA with copies of the format and content of data and other documentation and records as described in earlier sections of this document. We will transition in an orderly manner without service disruption. The work plan will include periodic updates.

1.7.2.2 Turnover of Paper Files and Documentation

FSSA will receive final copies of the paper files and financial paper records as described in previous sections of our response. Archived records will remain archived and will be turned over to FSSA's designee at the agreed-on transition date. Records that are not archived will be included on the transition inventory if they are required for continued delivery of services to eligible members, as agreed-on with FSSA.

Gainwell will make these records available for pickup by FSSA or its designee during the Transition phase. Financial records will be retained and made available to Gainwell in accordance with the contract, as necessary, to assist in confirming that Gainwell has properly fulfilled its undertakings according to the terms of the contract or other judicial or alternative dispute resolution proceedings.

1.7.2.3 Turnover of Documentation

Gainwell will provide FSSA with final copies of premium billing and collection services documentation in the electronic media format specified by FSSA. This documentation includes the documents provided in earlier sections of this plan. These records will be available to FSSA or its designee during the Transition phase.

1.7.2.4 Transition Training

Gainwell will provide FSSA or the successor with business operations training. On completion of training, we will update the training plan and submit the results to FSSA's training liaison for final sign-off. Training will begin 6 months before the end of the contract or the contract extension and be completed 2 months before the end of the contract or contract extension. Gainwell will assess training needs with FSSA and the successor to determine the type of training needed and the number of people to be trained. The final training plan will be submitted to FSSA for review and approval.

1.8 Resolution of Transition Issues

Identified transition issues will be tracked, resolved, and reported in Project Workbook and the Issue Management System. Gainwell will use issue and risk tracking logs that include the following:

- Unique identifier for reference and tracking
- Date the potential problem was identified
- Description of the problem

- Probability or likelihood of the problem occurring
- Potential impact of the problem on the project were it to occur
- Priority dealing with the problem
- Status of the problem (open, accepted, or closed)
- Indication if a risk management plan needs to be created

Gainwell will work with FSSA to provide proper coordination of transition activities that affect financial, banking, accounting, and operations for the contract. Transition plans to support the cutover and transition of operational responsibilities will be developed in cooperation with FSSA and its designee. Issues that are identified will be addressed promptly.

2 Contract Closeout Services

Gainwell will continue to function as the premium billing and collection services provider during the performance and retention period of this contract. Our staff members will provide reliable billing and payment processing along with online reporting capabilities to assist FSSA in meeting special fund management reporting needs until contract termination.

Reconciliations must be completed routinely during operations, and it is critical that a final accounting at contract closure confirms the integrity of the accounting records for the contract.

3 Financial Reconciliation

FSSA will benefit from Gainwell's financial professionals who bring extensive knowledge and experience to support accurate and timely financial reconciliation for the CHIP and M.E.D. Works programs. The Financial Operations Team will continue to be responsible for the transaction recording, tracking, and reporting requirements related to performing premium billing and collection services for FSSA during the Transition phase.

To support these functions, the Financial Operations Team will provide local Gainwell accounting and reporting staff, policies, and procedures to maximize consistency, accuracy, and efficiency. Timely and accurate reporting is essential for FSSA's confidence in program transition. We use consistent procedures to guide our staff in final reconciliation of banking and fund management processes during the Transition phase.

4 Post-Transition Reporting

Gainwell will prepare a final written assessment of our perceived contract performance during contract closeout services. Following the turnover of contract operations to FSSA or a new vendor, Gainwell will provide a Transition Results Report, the outline and format of which will be approved by the State in advance. This comprehensive report will present FSSA with the final completion status and results of each task identified in Gainwell's transition plan. FSSA can use this information to validate and approve completion of the transition portion of the contract. For each transition activity identified, the report will present the final completion status and results. Transition will not be considered complete until FSSA receives this document.

5 Appendix: Transition Manager Qualifications

The transition manager must have the following qualifications:

- Strong communication and organization skills
- College degree or equivalent experience
- At least 1 year of recent premium vendor experience.