RFP 22-68785
TECHNICAL PROPOSAL
ATTACHMENT F

Please supply ***all*** requested information ***in the yellow-shaded areas*** and indicate any attachments that have been included. Document all attachments and which section and question they pertain to.

2.4.1 Pharmacy network

Describe your existing pharmacy network in Indiana State or your ability and experience in developing other statewide pharmacy networks.

MC-Rx (previously ProCare Rx) has managed the retail pharmacy network for the Indiana ADAP program since 2007. The network includes nearly all retail and Specialty pharmacies in the State of Indiana. Our network for the ADAP program (including MDAP, HIAP and HIP) includes the Eskenazi Health pharmacy group, Walgreens, CVS, Kroger, Walmart, and Meijer. We also contract with all of the major Pharmacy Services Administration Organizations (PSAO's) representing the independent pharmacies in the State.

The top ten chain and PSAO pharmacies in the State fill over 99% of prescriptions for the ADAP program. Over 60% of program prescription dollars are filled by eight individual pharmacies including three Eskenazi pharmacies, Methodist Pharmacy, Walgreens pharmacy in Indianapolis, Damien Pharmacy, Healthy U Rx and Medical Park Pharmacy.

MC-Rx has exceptional experience in building pharmacy networks to support our thousands of customers. In fact, we currently operate hundreds of unique networks including statewide networks. Our network team is experienced in identifying coverage gaps for pharmacy networks and recruiting pharmacies to provide full access to our clients and customers. No coverage gap has been identified for Indiana ADAP.

Furthermore, our Pharmacy Network team works closely with the network regarding operational issues as they occur. We have frequent interaction with the pharmacies regarding the three Coordination of Benefit programs (MDAP, HIAP and HIP) to work through the processing requirements for the specific codes necessary to meet the program requirements.

Our Pharmacy Network team rapidly responds to any request by a pharmacy to enter the Indiana ADAP program. Pharmacy agreements are typically sent the same day or within one business day to a requesting pharmacy. New applicant pharmacies then must meet MC-Rx's stringent credentialing standards for licensure, insurance and operational requirements prior to inclusion in the Indiana ADAP network. The application, review and network update process typically takes less than 5 business days.

If you currently have a network of pharmacies in Indiana State, please include the complete list of pharmacies.

Please see the attached exhibit “2.4.1 – Indiana Pharmacy Network”.

Describe your ability to provide a mail order option for clients.

Patients have ease of access and affordability by being able to fill their prescriptions through mail order. There is no need for them to make time to commute to a brick and mortal retail facility; their prescriptions are mailed promptly with no inconvenience to them. IDOH can see advantageous savings when they allow their clients to have the ability to use our mail order service. PPC guarantees the integrity of all drugs and ensures your clients receive quality products and services at a great value on every prescription order. We believe owning and operating our own mail order and specialty pharmacy gives us better control in managing our IDOH’s prescription benefits at a lower cost, which allows us to offer the highest level of service to our IDOH and their clients in turn. Our Patient Portal allows for quick online access to medication profiles and status of medication orders. We also offer text messages and email communication.

An analysis of high cost Specialty drugs for YTD 2021 shows a potential savings to IDOH of over $440,000 annually based on the pricing offered in this RFP response. We can work with IDOH to implement the programs and outreach to achieve the savings available.

Provide a description of how you communicate with pharmacies in your network when you need to inform them of significant events.

For pharmacy notices and bulletins, we send out fax and/or email notices to the pharmacy network. If the notice requires multiple submissions, we will send out as required. In some cases, we will reach out by phone to the major chains or significant individual providers to provide education regarding processing issues to mitigate network disruption.

In the past, we have communicated with INADAP pharmacies by phone to provide education and assistance with COB claims processing.

2.4.2 Drug cards

Describe your ability and experience in preparing prescription drug cards. Include a description of how you ensure that eligible clients can get their drugs even if they do not have such a card.

Unified Group Services utilizes an integrated ID card that includes information on the medical program as well as the pharmacy information so that clients only have 1 card to access benefits under the HIV programs. ID cards have been a necessity since Unified Group Services was started over 25 years ago. While a client may not have a physical card in hand, our eligibility is up to date with MC-Rx so that a client can get a

prescription filled. We also have an electronic copy of the ID card available at UnifiedGrp.com that can be printed off and used immediately while the laminated card is in transit.

2.4.3 Third-party administration

Describe your ability and experience in providing electronic pharmacy claims processing.

MC-Rx's internally developed and maintained real-time claims processing system has integrated all retail, mail order, and paper claims since 1994.

Provide a description of your ability to do online adjudication and split billing, and your backup procedure for pharmacies that are unable to do submit secondary claims electronically.

Our system includes, but is not limited to, establishing drug coverage algorithms at plan, pharmacy, physician, and client level, or any combination thereof. The system allows for sophisticated plan benefits, automated clinical step edits, multi-tiered enrollment, flexible copay structures, variable formularies, multi-level administrative fees, variable card production, and many other features that can be demonstrated. In addition to flexible plan designs, the online system, which is integrated with our Customer Care Center (pharmacy client help desk), provides approximately 1,500 edits during the adjudication of each claim, including real-time concurrent drug utilization reviews that are based on First DataBank DUR Clinical Modules as set up by IDOH override parameters.

We can provide assistance if the pharmacy has received a rejection on the secondary claim. The pharmacy would call into MC-Rx's Help Desk and work with one of our agents to identify the reason for rejection and discuss next steps.

Regarding a backup plan for secondary claims, we would be able to do a DMR by manually keying a secondary claim on behalf of the pharmacy.

Describe how you monitor billings to assure non-duplication and proper split between primary and secondary payers.

MC-Rx's Plans can be set up to allow Primary Only, Secondary Only, or both Primary and Secondary. If the client should only be submitting a secondary claim to MC-Rx, the IN ADAP eligibility file indicates what type of claims can be submitted. Therefore, plans can accept both primary and secondary. The IN ADAP eligibility file drives what is accepted for the client COB codes (COB 2 or 8; or COB 8, or COB 0, 1, 3, or 8).

For the medical claim administration part of the program, Unified Group Services claims processing system has edits in place to flag duplicate submitted claims for review. Any claims for the medical programs where IDOH is the secondary payer, we pend those claims until we receive the primary carrier's EOB that shows how much they paid to then determine the amount for IDOH to cover. Unified's claims account manager continually helps educate clients & providers on how the program coordinates and how all other coverage options should be billed by the provider first before the IDOH program is utilized.

Describe how to monitor payment of allowable vs. unallowable costs, including reversal or denial of unallowable claims.

Unified's claim processing system is customized to only allow eligible services under each program. If a service is billed by a provider that is not covered, it is denied. If additional information is provided regarding primary coverage or additional services provided, that information is reviewed. Upon review of that information if a reversal is needed, we can process that type of claim. If refunds are needed from the provider, Unified will issue a refund request to the provider to recapture the funds. The provider then will bill the appropriate primary coverage for payment. The is a necessary part of the administration of the programs to help ensure that IDOH is the payer of last resort.

Describe your experience administering services designed to "wrap around" or complement Medicaid and Medicare Part D benefit plans.

Since the beginning of the Medicare Part D program, our organization has provided the administrative services for the unique needs of our employer groups and the customized benefits they had for their employees. Our current Medical Part D clients include a MA – PDP, self-funded employer groups and Taft Hartley Welfare Funds and our own fully insured small group EGWP program. Our services include all Medicare Part D administration, reporting, claim processing, formulary management, PDE reconciliation, and pharmacy network management.

We have the capability to administer any number of plan designs including wrap options, depending upon the needs of the customer/group. This allows clients to extend various co-pays (flat, split, percentage, tiered), formulary, and deductible (front-end and annual maximum amounts) to your clients. Currently, we have clients that offer their members multiple levels of pharmacy benefits, based upon client's employee retirement date. Each level of benefits offers different co-pays, with the lowest co-pay being offered to the members who retired the earliest. Managing benefits of this magnitude is not an obstacle for us; in fact, it is the norm. We will work with your organization to develop a plan design that best meets your needs and CMS minimum requirements. On a self-funded basis, we allow our clients to cover any medications they want to provide their membership. The client must remember that CMS non-covered medications do not count towards any accumulators and are not considered allowable towards any subsidy calculations for the Med D program. Our organization can provide the current benefits program.

For the MDAP program, we can coordinate as secondary payer for IDOH to capture the client owed amount which would then be processed for payment by IDOH.

Describe your ability and experience in fee-for-service claims processing. Describe your ability and experience in adjudicating fee-for-service claims.

Unified has a long history of fee-for-service claims processing since that has been the prevalent billing method by medical providers. We can accept already repriced claims from a network (like is currently done by Encore Health Network for the EIP program) or we can utilize a fee schedule maintained in-house and reprice the claims in our claims system.

2.4.4 Payer of last resort

Describe methods used to ensure that the HIV Services Program will be the payer of last resort.

MC-Rx process is such that for plans or individuals set up with COB restrictions, if primary payment is not received, messaging is sent back to the submitting pharmacy to seek payment there first. This helps ensure that for MDAP, HIAP, & HIP that the primary insurance provider is billed & processed first before IDOH for compliance as payer of last resort.

Plans can be set up to require primary payer information submitted on the claims transaction before allowing a secondary or tertiary payer.

For medical claims processed by Unified Group Services, any client where other primary coverage is in place, we will pend that claim & not process it for payment until the primary EOB is received to determine how much client responsibility is. Then that is the amount that IDOH will cover. If a client is on the EIP program, if we get claims that indicate a primary insurance carrier could be involved, we will pend that claim. Unified claims account manager will reach out to the provider & our contacts at IDOH to verify if there is in fact primary coverage that should be billed. If there is a primary insurance carrier, then Unified will work with IDOH to help get that client moved over to the appropriate program.

Unified's claims account manager continually helps educate clients & providers on how the program coordinates and how all other coverage options should be billed by the provider first before the IDOH program is utilized. If there is a primary insurance carrier, then Unified will work with IDOH to help get that client moved over to the appropriate program.

How will participants be screened for other insurance coverage, and how will IDOH be notified of any duplicate coverage discovered?

For pharmacy claims processing, the clients are placed in individual plans that restrict the COB coverage per the IDOH requirements. If clients have COB restrictions, they must come over on the eligibility file or be entered manually on the client record. If COB restrictions are present for the client, claims will process according to the information provided. Plans can also be set up to be COB plans only. This would mean that any claim processed to the plan must have the COB requirements present or the claim would reject.

For the medical claims, if a client is on the EIP program and we get claims that indicate a primary insurance carrier could be involved, we will pend that claim. Unified claims account manager will reach out to the provider & our contacts at IDOH to verify if there is in fact primary coverage that should be billed. If there is a primary insurance carrier, then Unified will work with IDOH to help get that client moved over to the appropriate program.

Describe how overpayments will be recovered.

When an overpayment issue is brought to our attention, MC-Rx will work with the participating pharmacy to have the claim reversed and resubmitted to the primary payer. The result of the process will reflect on the next billing cycle.

Unified Group Services will submit a refund request to the medical provider and provide information of why a refund is being request. Then once the refund is received, it is credited on the IDOH claims funding request.

2.4.5 Enrollment management

Describe the Respondent's ability to accept electronic data interchanges to manage enrollment records (new enrollees, address changes, and terminations). Individual updates may be exchanged as often as daily; routine updates will be exchanged weekly, and full enrollment reconciliation will occur monthly.

Currently, Unified receives all enrollment electronically through our UnifiedGrp.com secure benefits portal. The enrollment is submitted directly to your Dedicated Eligibility Specialist. She enrolls the client and requests an ID card that will get mailed to the client or the applicable care coordinator.

Unified does have the ability to accept electronic eligibility files, and we would be glad to explore this option with IDOH should they wish to change the procedures.

Describe how the Respondent will provide IDOH with the on-line capability to access or modify enrollee eligibility data and to generate statistical reports on enrollment.

The UnifiedGrp.com benefits portal is customized based on the demographic information specific to IDOH clients. It is a seamless process from data entry to our internal dedicated eligibility contact. Due to our integration with the PBM, the client is also enrolled into their system for applicable Rx benefits. Unified can provide eligibility reports to IDOH as needed.

Describe if the Respondent can process enrollment charges within one (1) business day. Changes may be initiated by IDOH, Marketplace carriers, Medicare, or the enrollee and may include address, name, and program status changes. Processing includes notifying IDOH if IDOH did not initiate the change.

The average turnaround time from receipt of enrollment to updating the information in our system is 24-48 hours, typically enrollments are processed within 24 hours.

Provide the Respondent's ability to distribute a single enrollee benefit card to each eligible enrollee within two (2) business days. Provide examples of benefit cards developed in the past.

Once an ID card is requested by the eligibility specialist, it is ordered through our vendor and an electronic copy of the ID card is available on UnifiedGrp.com. The hard copy card is mailed directly to the client or the applicable care coordinator. On average hard copy ID cards are requested within 48 hours after receiving the enrollment.

Included in this submission are examples of ID cards for each of the programs that Unified has been administering.

2.4.6 Formulary

Describe your ability and experience in managing a formulary that includes specific drugs and classes of drugs. Include a description of how you ensure routinely capturing FDA decisions that affect approved classes of drugs.

MC-Rx has experience managing the IDOH closed formulary. There are currently 49 antiviral drugs and an additional 225 drugs in other therapeutic classes covered. If the drug is not listed on the formulary, it is not covered and will reject at the point of sale.

IDOH only covers FDA-approved medications and pays 100% for the prescriptions on formulary.

IDOH typically sends formulary updates to MC-Rx two to four times annually. The full formulary is sent over with additions and deletions specified. The changes are implemented in our system and tested for accuracy. This entire process is turned around in 7-10 business days, depending on the volume of changes requested.

2.4.7 Provider network

Describe the Respondent's plan to ensure that potential EIP providers accept the program's reimbursement as payment in full.

Unified Group Services claims account manager will engage with providers to educate them on the EIP program and what is covered & not covered. This helps the provider to know how to manage the payments in their system to close out the claims & not bill the client. If the question from the provider relates to discounted rates from their contract with Encore, Unified will engage Encore's provider relations team to reach out to the provider & educate them on the process to account for the payment and mark it payment in full.

Describe the Respondent's plan to work within each Marketplace carrier's network of providers and pharmacies to coordinate HIAP benefits.

Unified will request copies of the Medicaid EOB's to determine what the client's out of pocket expense is that would be eligible for coverage under the IDOH HIAP program.

MC-Rx's system is set up that pharmacies are prompted to submit prescription claims to the PBM for the Marketplace policy first before it being processed by MC-Rx under the HIAP benefits.

Describe the Respondent's plan to work within the various Medicaid plan guidelines for participating providers.

Unified will request copies of the Medicaid EOB's to determine what the client's out of pocket expense is that would be eligible for coverage under the IDOH HIP program.

Describe the Respondent's plan to work within the various Medicare Part D plan guidelines for participating providers.

Since the inception of the Medicare Part D program, MC-Rx has acquired 15 years of significant and valuable expertise in all operational and regulatory areas. This has resulted in proven outstanding results obtained on behalf of our customers. MC-Rx's expertise in working in the Medicare environment includes:

Formulary Management:

- The development of formularies based on USP guidelines and CMS requirements established in Chapter 6 of the Prescription Drug Benefit Manual.
- Compliance with CMS in reviewing new medications and line extensions and all CMS protected therapeutic classes promptly
- The development of all protocols and the documentation required to be submitted to CMS to justify each protocol. MC-Rx has been very successful in documenting all necessary information to obtain CMS immediate approval for almost all protocols submitted.
- Submission of all files directly to CMS with a very high approval rate percentage.
- Annual review of all products within each therapeutic class.
- Negotiation with pharmaceutical companies to achieve the lowest net cost in each therapeutic class.
- MC-Rx's clinical department personnel participates in all CMS Part D user calls to keep up to date on all changes.

Plan Setup And Benefit Design:

- MC-Rx has gathered expertise as a consultant to our customers to ensure that all plan designs meet CMS requirements and that set up is made according to submitted bids.

- MC-Rx supports our customers in identifying the impact of their plan designs on PDE reporting and CMS reimbursements.

PDE Management:

- Understanding of CMS requirements and supporting our customers in meeting CMS requirements and achieve operational and financial goals.
- Providing tailor-made reports to our customers for transparency and oversight.
- Guaranteeing over 99.7% PDE acceptance rate.
- Managing all the reprocessing necessary in a timely fashion to produce accurate PDEs, according to CMS requirements.
- Cyclic and ad-hoc PDE cycles to comply with CMS submission requirements.

Pharmacy Network Development and Contracting:

- Ensuring that all pharmacy network service contracts are in compliance with CMS requirements.
- Education of our pharmacy network, through on-site visits, among others, to ensure they comply with all CMS rules and regulations (e.g. verification of exclusions lists, CMS-10147 forms, etc.)
- Providing CMS with all files required and maintaining an updated pharmacy network list.
- Supporting our customers and the National Benefit Integrity – Medicare Drug Integrity Contractor (NBI-MEDIC) in any FWA investigation required.

Call Centers:

- Maintaining all call centers statistics in compliance with CMS requirements.
- Providing uninterrupted, high quality service in “peak” months each year.
- Continuous training to MC-Rx’s call center personnel to keep them informed of all changes.

Reporting:

- Expertise in developing CMS-compliant reports (e.g. Reporting Requirements, audit universes, Transition Monitoring, etc.).
- Maintaining and updating all reporting requirements, as they change.
- Providing our customers with all reports required by CMS accurately and in a timely manner.

2.4.8 Technical support

Describe your ability and experience in providing technical support to program staff, pharmacies, and clients.

The Program staff has direct contact with their assigned Account Manager, as well as the Manager and Director or Client Services. The Account Management team supports the Program staff and provides assistance for system user access, reporting needs, and any drug coverage exceptions (lost/vacation overrides). Additionally, the Account Manager handles any help desk ticket escalations for a resolution by contacting the Program staff for consult and approval for overrides and/or calling pharmacies to assist with claims adjudication, if needed.

The Customer Care Center in Gainesville, GA is open 24 hours, 7 days a week, and 365 days a year at 855-828-1484 or a specially assigned toll-free number if a client needs its own number. We also have a facility Miramar, FL.

For customers and pharmacies, through our internally developed and maintained Help Desk Manager tool, we have the ability to track each call received and report on the reason, type of caller, first call resolution rate, and other detailed information regarding the calls. Daily, weekly, and monthly reports are created with each call getting assigned a 'category' number that helps us monitor call resolution by category type and resolve any CSR training issues or overall client concerns connected to any one client.

Unified's team that works on the IDOH programs have years of experience to help educate the staff, clients, and providers about what is covered under each program. Anytime our team has questions, see a common issue with clients or providers, we notify the IDOH staff about it and see what adjustments may be needed for the program.

We are also available to come meet in person with the IDOH team to talk about how the program is running & ways to continually improve it.

Provide a description of the levels of service you provide at various times during the day. For example, describe the level of service you provide during business hours versus the type of support you provide during non-business hours including your holiday hours.

MC-Rx Help Desk to support clients and pharmacies is available 24x7x365, including all holidays. The same standards for speed of answer, call blockage rate, etc. apply regardless of the time of day. Staffing is adjusted to assure service levels are maintained to meet the requirements of our clients.

For technical issues, system security is managed by an IT team that monitors user access, intrusion, detection, system hardware issues, software maintenance, and other issues. The team is available 6AM-8PM ET in-office and by cell phone after-hours.

After-hours notification is either via automated alerts or via phone call to our 24-hour call center support. The call center support staff will then notify the after-hours IT contact of the issue.

Once the after-hours IT person is notified of an issue, they will log in to determine the cause and which systems are impacted. They will make the determination whether they can resolve the issue or if it needs to be escalated or assigned to another team for resolution.

Unified Group Services has a live answer phone system available 8:00 am – 5:00 pm EST Monday through Friday. Our service model is designed that if there are questions about eligible or claims you will get a live person to answer the phone. The same person that manages the claims & eligibility will handle phone calls too, so you do not have to be passed around to different departments. UnifiedGrp.com is available 24/7 and clients can email the claims account manager with questions about claims at any time.

Describe your ability to keep records on problem resolution.

We have processes and procedures that ensure that once an issue is identified, it is clearly documented, including the root cause, who identified the issue, how the issue was identified, when was it reported, as well as an in-depth analysis to find what caused the issue. Additional precautions are taken to ensure that the issue is contained. Steps are put in place immediately while keeping thorough documentation and communicating frequently with all parties during this process. Any necessary changes or modifications are made to guarantee that there is no repeated occurrence, which includes continuous review and regression testing across the board. Final documentation and all the processes are sent to the client with constant communication until the conflict is fully resolved, and the client no longer has comments or concerns.

2.4.9 Data system

Describe your ability and experience in creating and managing data systems that receive client eligibility information from the program of origin and use it for payment information with pharmacies.

Eligibility files are created by the client in a pre-determined format and placed on our sftp site. They are imported into our system and used for adjudication. At the end of every billing cycle claims are extracted and provided to the client in a report that contains the card ID and patient name, that were previously provided by the client, along with other claim details.

Provide a description of how you ensure that you enter client eligibility information on the same day in which you receive it.

MC-Rx: The eligibility process can be automated so that upon file drop processing will start within 5 minutes and continue until the file is completed.

Unified: As enrollment is entered online to UnifiedGrp.com, notification is provided to the eligibility specialist to review the submission. The average turnaround time from receipt of enrollment to updating the information in our system is 24-48 hours, typically enrollments are processed within 24 hours. If additional information is needed to validate program eligibility may need to be requested from IDOH.

2.4.10 Monthly, quarterly, and annual reports

Describe your ability and experience in creating reports that describe monthly user activity and prescription drug costs.

Monthly and quarterly reports include a wide variety of utilization, financial, rebate, and performance reports. IDOH can either request a customized report that turns into a weekly, monthly, or quarterly report or extract the information themselves using our online reporting tools. We will commit to provide any report to you that you do not find in

our report library. All reporting needs are discussed upon implementation.

MC-Rx provides a daily claims file and bi-monthly claims reports. The bi-monthly claims reports include customized fields used for state rebate reporting requirements. MC-Rx processes and loads daily eligibility files and produces the output reports specific to the file loaded from each import. These files and reports are posted to our STFP/FTP client accessible site. Additionally, we have provided and can generate at any scheduled interval a client listing for all active clients, reject claims tracker, and drug class ad hoc reporting.

Provide a description of your standard reports, if any, and your ability to create custom reports.

MC-Rx: Our systems are extremely flexible in extracting any data, grouping, categories, etc. from our customers' data warehouse. We will commit to provide any report to you that you do not find in our report library, but all of our customers' reporting needs are discussed upon implementation to ensure that they are getting all the information they need from our reports for their personal and auditing needs. MC-Rx has 4 basic levels of reporting capabilities:

Monthly/Quarterly – MC-Rx offers a reporting package on a cycle, monthly, and/or quarterly basis, as applicable to the services provided. At a client's request, we deliver the selected reports electronically through our secure FTP site agreed upon by both parties at no additional cost.

Reports Portal – MC-Rx's Reports Portal is available for claims queries right from our customers' desktop or laptop. The Reports Portal contains a library of useful list reports that customers can generate at their convenience, which includes real-time claims data. This reporting tool is included in our basic services and at no additional cost.

Ad-Hoc Reports – MC-Rx can provide ad hoc reports for those situations where a monthly/quarterly report or Reports Portal report does not exist.

Zero-!n – MC-Rx's Zero-!n is an interactive query tool with a point and click graphical interface which customers can use for specialized analysis of their prescription programs. With Zero-!n, a client can analyze all of their claims by selecting time frames, clients, doctors, drugs, pharmacies, and many other data elements from their prescription data. The interface offers charts, graphs, columnar tables and easy-to-use flexible selections. Data from Zero-!n can be exported to Word documents, integrated with PowerPoint presentations, and transferred to Excel for further customization and integration with external data. Two Zero-!n licenses are included in the administrative fee.

Unified Group Services provides the following standard reports:

Weekly – Funding claims detail report of the amounts to be paid and which type of service that amount falls under. This helps IDOH track up front how much goes into each reporting category for ADR & RSR reporting requirements.

Monthly – Summary reporting by program of dollars spent & number of clients in each

program.

Quarterly – Prescription Drug CLD Report, Rebate Report, & Gilead CLD report so that IDOH can efficiently submit drug claim data to drug manufacturers so rebate money can be released to IDOH for funding the programs.

Annual – Detailed reports for ADR/RSR report submissions and WICY reports

Ad-Hoc – We have the capability to build custom reports to capture any data that is billed on a medical claim or submitted with eligibility enrollments.

All reporting generated by Unified Group Services is included in our administration fee, we do not charge for report requests.

2.4.11 Monthly payment

Describe your ability and experience in providing payment upfront and then timely submitting for reimbursement later.

MC-Rx's pharmacy contracts govern the payment guidelines & processes. MC-Rx generates a bi-monthly invoice of the prescription drug activity for each program. This invoice is sent to Unified Group Services to process and break out drug cost vs per script administration fee for submission to IDOH for payment. Once IDOH releases the funds to Unified Group Services, those funds are paid to MC-Rx. MC-Rx then provides the reimbursement to the pharmacies as outlined in their contract.

Provide a description of how you ensure that you request reimbursement only for valid claims; include detail about your claims checking processes that eliminate duplicate or invalid claims.

The claims system has built in edits to identify potential duplicate claim submissions which are set up to automatically deny unless additional information is provided to substantiate it being a valid claim.

Unified also audits claims prior to release on the funding request submitted to IDOH as another level of checks to help make sure only valid claims are submitted.

2.4.12 Client confidentiality

Describe your ability and experience in assuring client confidentiality and any security or confidentiality breaches your company experienced in the past five years.

MC-Rx has never had a security breach into our systems.

Encryption controls include SSL/TLS for web application and APIs, WPA2 Enterprise for Wi-Fi communications, IPsec for VPN tunnels, SFTP for secure file transfers. Every client connection is secured by 128-bit SSL encryption via HTTPS and protected by SSL

via the web servers. MC-Rx also uses hardware and software filters that block any non-secure connections between client devices and web applications. All data transfers require secure FTP login, encryption or key tags for appropriate transfer. MC-Rx systems maintain the highest security through multiple levels of password protection. Security is provided at the system, server, folder, and application level and is maintained by our IT department. For any other entities to access data in any way, a Business Associate agreement is required.

MC-Rx maintains strict compliance with the HIPAA Privacy and Security Rule. MC-Rx and its employees may use and disclose protected health information (PHI) for Payment, Treatment, and Health Care Operations (PTO) only if we are dealing directly with the client. We may release PHI only if the patient has specifically signed and executed a "Consent for the Use and Disclosure of PHI Form" that grants MC-Rx or its customers and employees the right to use and disclose PHI to carry out PTO. However, this consent only allows MC-Rx or its Customers and its employees to use and disclose the "Minimum Necessary" amount of information required to complete the desired task.

Within the MC-Rx facility, the floor plan is configured so that passersby walking around the facility cannot view the screens of our associates. Customer Care Center associates are also provided voice sensitive headsets so that they can have a private conversation when discussing sensitive information with pharmacy or client callers. Simple items from the shredding of peripheral paper that might contain PHI to destruction of mistakenly printed ID cards are all carefully monitored within the Customer Care Center environment.

Unified has not had any breaches of client confidential information. The data stored for the IDOH programs are in group numbers within our claims system that we limit internal access to only those with direct tasks relating to administering those programs. Every employee signs off on adhering to Unified's HIPAA policies and strict confidentiality. We have ongoing, quarterly HIPAA training sessions with attendance documented for all employees. We are very diligent on maintaining confidentiality & security. We have extensive HIPAA policies in place to govern & monitor system access, data use, & compliance.

Describe how you protect client information from being used for commercial purposes.

The data generated by the Program is the client's data and any use of that data is specifically addressed and limited by the terms and conditions included in the Client Service Agreement ("CSA"). The client data use limitations set out in the CSA are implemented as part of the overall plan specification that is programmed into the claims processing system and subject to multiple quality control reviews prior to the go-live date, as well as periodically thereafter. There have never been instances in which client data that is proscribed against further commercial use (such as in pharmaceutical manufacturer rebate programs) as any such commercial use includes separate quality control processes against the plan specifications.

Employees with access to client information are subject to multiple non-disclosure and HIPAA attestations and ongoing training, as well as to systematic controls to ensure that client information access follows the HIPAA minimum necessary standards.

The data stored by Unified Group Services is the property of the IDOH and it is not release for any commercial purposes. Only those authorized on the IDOH HIPAA roster to review PHI has that level of access.

2.4.13 Logical and operational security controls

What is the highest security classification of your system?

MC-Rx's information classification scheme includes the following:

- Personal – includes user's personal data, emails, documents, etc. This policy excludes personal information, so no further guidelines apply.
- Public – includes already-released marketing material, commonly known information, etc. There are no requirements for public information.
- Operational – includes data for basic business operations, communications with vendors, employees, etc. (non-confidential). The majority of data will fall into this category.
- Critical – any information deemed critical to business operations (often this data is operational or confidential as well). It is extremely important to identify critical data for security and backup purposes.
- Confidential – any information deemed proprietary to the business.

Describe your ability to protect authentication credentials, and the information collected, processed, transmitted, or stored. Include a description of the security design and controls to:

- Restrict access to data.
- Protect and control data transmissions.
- Protect the system against unauthorized intruders.

MC-Rx's system has significant physical and electronic data security access in place that meet the security access and intrusion detection levels for URAC and NCQA accreditation as well as SSAE16 level audits.

Logins to the virtual environment are logged and said logs are audited on a regular basis.

All VMs that contain sensitive information are running endpoint protection software with host-based IPS/IDS.

All of our production data is stored with the same level of security and protection.

Describe the operational and logical network security controls.

MC-Rx develops and maintains all systems. Our systems operate on an N tier platform. For all systems, there is a database layer and a presentation layer.

Our systems have never experienced a security breach. System security is managed by

our IT team that monitors user access, intrusion, detection, firewall pinging, virus threats, and other access threats. The team controls access to virtual drives, servers, and specific folders. Program security is controlled by our IT team or the customers themselves.

MC-Rx maintains strict compliance with the HIPAA Privacy and Security Rule. MC-Rx's systems maintain the highest security through multiple levels of password protection. Security is provided at the system, server, folder, and application level and is maintained by our IT department. All data transfers require secure FTP login, encryption, or key tags for appropriate transfer, and MC-Rx does not permit the faxing by our employees of any PHI, even to our customers. For any other entities to access data in any way, a Business Associate Agreement is required. MC-Rx and its employees may only use and disclose protected health information (PHI) for Payment, Treatment, and Health Care Operations (PTO) if we are dealing directly with the client. Additionally, all employees must complete HIPAA compliance training and pass a HIPAA compliance test with 80% or higher upon hiring and once a year thereafter.

The overall ProCare Rx enterprise systems comprise three major layers:

- Transaction Management (commonly referred to as transaction switching)
- Pharmacy Claim Adjudication Engine
- Data Warehouse

Unified Group Services Policy

Access to electronic protected health information (ePHI) will be authorized, established, maintained, and modified based on the minimum amount of PHI necessary for individuals to perform their jobs.

Procedure

1. A member of the workforce will not be granted access to ePHI until the IT form is filled out by the supervisor of the workforce member. The supervisor will review the individual's job responsibilities and determine that access to ePHI is required for the individual to perform his or her responsibilities. Such review will be documented on the IT form and maintained during the time the individual is a member of Unified Group Services' workforce.
2. Authorization to access ePHI will be limited to the documented determinations of the minimum necessary amount of ePHI (according to the Privacy Rule) needed by the individual to perform his or her job.

a. Notice will be sent to the HelpDesk, including a New Employee Checklist, to establish security and access to ePHI.

3. After access privileges have been authorized, a user account will be established that enables the individual to access ePHI and the information systems according to the review performed in sections 1 and 2 of this Policy.
4. For individuals who have access to ePHI, documentation will be maintained of all user accounts and authorized access privileges for at least seven years.
5. On an annual basis, the Security Officer along with Supervisors will review the access rights and user accounts of all individuals who have access to ePHI to ensure continued appropriateness of accounts and levels of access.
6. For individuals who have access to ePHI, access privileges will be modified or revoked whenever an individual's job function or access needs change. Modifications to user accounts will be made with appropriate authorization.
7. For members who have access to ePHI, access privileges will be revoked when a

user is no longer employed. This revocation will occur on the effective date of the individual's end of employment or sooner if warranted by circumstances.
a. Notice will be sent to the HelpDesk, including Employee Checklist, as soon as the change or termination is known. This will be kept for seven years.
8. Removable media access will be controlled by logging information out of controlled storage location.

Describe the vulnerability management practices.

Privacy and security, including those under HIPAA and HITECH (for PHI) are included in the external audit process, which occurs multiple times per year. In addition, there is a third-party external security and intrusion test conducted annually. The records are retained for at least three years per our retention policies.

Unified Group Services works with an outside IT security auding firm for system testing and review.

Describe the log collection and management practices.

MC-Rx: We maintain logs of access to the system through system security and login files, as well as log files for each stored data table that is accessible to any user. Logs from IDS/IPS, Endpoint Security are sent to LogRhythm (SIEM) for processing. LogRhythm will generate notifications and send to security personnel on security events triggered by network security devices.

Unified Policy
Information system activity records will be reviewed when reasonable and appropriate to prevent, detect, correct, and contain security violations.
Procedure

1. The Unified Group Services HIPAA Security Officer will coordinate the review of information system activity records.
2. Unified maintains an internal security control program, which is coordinated by the IT department. This program compliments the electronic access privilege (user authentication) process and acts as a deterrent to internal abuse by making users aware that audit trails, file access reports, and security incident tracking reports can be produced, reviewed, investigated and then subject to applicable sanctions. Employees are reminded annually that records of information system activity can be reviewed. It is reasonable and appropriate that the audits are completed when there is just cause or suspicion of a security breach. The Privacy and/or Security Officer and supervisor of the user will review the audit to determine if the access of data was reasonable and appropriate.
3. Review of information systems activity provides an automatic trail or log or trace of user actions whenever sensitive or critical protected health information (PHI) is accessed or modified by a workforce member. Together, the audit log, file access reports, and security incident reports promote individual user accountability and allow Unified an ability to reconstruct significant events or

suspicious activities as necessary.

4. Documentation of the review of information systems activity for Unified includes:

   a. Business decision criteria used to define data selected for audit trail, file access report and security incident reports (by system, application, and/or user activity)
   b. Audit records in a retrievable and usable form that are archived on a routine basis.
   c. Mechanism to capture and track audit trails, file access reports, and security incident tracking reports
   d. Defined separation of responsibility between those security personnel responsible for administering the review of information systems activity functions and those who monitor the reports.
   e. Provision to maintain offline storage of audit logs, file access reports, and security incident reports in a secure manner and for a specified period of time.
   f. Use of intrusion prevention measures.

Describe your data encryption and key management practices.

Encryption controls include SSL/TLS for web applications and APIs, WPA2 Enterprise for Wi-Fi communications, IPsec for VPN tunnels, and SFTP for secure file transfers. Every client connection is secured by 128-bit SSL encryption via HTTPS and protected by SSL via the web servers.

MC-Rx also uses hardware and software filters that block any non-secure connections between client devices and web applications. All data transfers require secure FTP login, encryption, or key tags for appropriate transfer.

Describe the operational and logical controls used for remote access into the network and network systems.

Remote access is only granted to employees who have been permitted use by management, and it is associated with the employee's network credentials. Remote access is allowed via IPSec Virtual Private Network (VPN) or Remote Desktop Services Gateway protected by TLS encryption. Access is logged in our SIEM platform. Systems are interfaced with backwards compatible password requirements.

Employee remote access is limited to approximately 20 employees and is reviewed monthly. Access is reviewed and approved/denied upon hire and/or change of position.

Customers access MC-Rx's systems via the Internet. A sophisticated, redundant firewall has been implemented to restrict Internet access to only authorized personnel. A user identifier and password are required to gain access to the MC-Rx Network on which the applications are processed. Additional application-level security controls the functionality of a user's access and also limits the data a user may view or update. Application security logs provide an audit trail of user access. Client Services personnel use the System Manager application to maintain employee and remote user security.

Unified Remote Access is governed by a work at home policy and agreement that signed by each employee that is granted permission and access for this. Remote access is only through encrypted laptops or tablet devices set up and managed by Unified Group Services. Secure connections are only allowed from these devices and additional layers of passwords are utilized in addition to the normal system access credentials.

Describe your IT Risk Management practices.

MC-Rx conducts an assessment of risk, including the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits. Risk assessments are reviewed and updated weekly or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the secure state of the system.

A third-party assessment of all critical systems and security controls is conducted annually.

Unified Group Services works with an outside IT security auding firm for system testing and review.

Describe the practices for securing databases and application servers.

Customers and MC-Rx users access systems via the internet. A sophisticated, redundant firewall has been implemented to restrict internet access to only authorized personnel. A user identifier and password are required to gain access to the MC-Rx Network on which the applications are processed. Additional application-level security controls the functionality of a user's access and also limits the data a user may view or update. Application security logs provide an audit trail of user access. Client Services personnel use the System Manager application to maintain employee and remote user security.

System security is managed by our IT team that monitors user access, intrusion, detection, firewall pinging, virus threats, and other access threats. The team controls access to virtual drives, servers, and specific folders. Program security is controlled by our IT team or the customers themselves. We maintain logs of access to the system through system security and login files, as well as log files for each stored data table that is accessible to any user.

MC-Rx maintains strict compliance with HIPAA privacy and security rules and has written policies and procedures for administrative, technical and physical safeguards. Specific security policies and procedures may be provided upon request.

Describe the incident response practices.

A security incident, as it relates to the company's information assets, can take one of two forms:

- Electronic – This type of incident can range from an attacker or user accessing the network for unauthorized/malicious purposes, to a virus outbreak, to a suspected Trojan or malware infection.
- Physical – A physical IT security incident involves the loss or theft of a laptop, mobile device, PDA/Smartphone, portable storage device, or other digital apparatus that may contain company information.

Electronic Incidents

When an electronic incident is suspected, the company's goal is to recover as quickly as possible, limit the damage done, and secure the network. The following steps should be taken:

- Remove the compromised device from the network by unplugging or disabling network connection. Do not power down the machine.
- Disable the compromised account as appropriate.
- Report the incident to the IT Manager.
- Backup all data and logs on the machine, or copy/image the machine to another system.
- Determine exactly what happened and the scope of the incident
- Notify company management/executives as appropriate.
- Contact an IT Security consultant as needed
- Determine how the attacker gained access and disable this access.
- Rebuild the system, including a complete operating system reinstall.
- Restore any needed data from the last known good backup and put the system back online.
- Take actions, as possible, to ensure that the vulnerability (or similar vulnerabilities) will not reappear.
- Reflect on the incident.
- Consider a vulnerability assessment as a way to spot any other vulnerabilities before they can be exploited.

Physical Incidents

Physical security incidents are challenging, since often the only actions that can be taken to mitigate the incident must be done in advance. This makes preparation critical. One of the best ways to prepare is to mandate the use of strong encryption to secure data on mobile devices. Applicable policies, such as those covering encryption and confidential data, should be reviewed.

Physical security incidents are most likely the result of a random theft or inadvertent loss by a user, but they must be treated as if they were targeted at the company.

The company must assume that such a loss will occur at some point, and periodically survey a random sampling of laptops and mobile devices to determine the risk if one were to be lost or stolen.

Response
Establish the severity of the incident by determining the data stored on the missing device.

Loss Containment
Change any usernames, passwords, account information, WEP/WPA keys, passphrases, etc., that were stored on the system. Notify the IT Manager. Replace the lost hardware and restore data from the last backup. Notify the applicable authorities if a theft has occurred.

Notify the executive team, legal counsel, and/or public relations group so that each team can evaluate and prepare a response in their area.

Review procedures to ensure that risk of future incidents is reduced by implemented stronger physical security controls.

Notification
If an electronic or physical security incident is suspected to have resulted in the loss of third party or customer data, follow applicable regulations and/or industry breach disclosure laws.

Additional security policies and procedures can be provided upon request.

Describe the physical, environmental, operational, and logical controls used to secure the data center.

The facility is protected by electronic access control 7x24. All entrances are under video surveillance 7x24, with access provided to employees through the use of a fob. Fobs can be programmed so that employees can only access the facilities at given times, or anytime (7x24), depending on job function. Data center access is restricted to necessary personnel only and is protected by access control and 7x24 video surveillance.

Customers and MC-Rx users access systems via the internet. A sophisticated, redundant firewall has been implemented to restrict internet access to only authorized personnel. A user identifier and password are required to gain access to the MC-Rx Network on which the applications are processed. Additional application-level security controls the functionality of a user's access and also limits the data a user may view or update. Application security logs provide an audit trail of user access. Client Services personnel use the System Manager application to maintain employee and remote user security.

MC-Rx access controls are used to limit user access to only the data and functions for which they have been authorized. Each user is provided a unique username and password that securely logs every addition or modification made in the system. There are multiple access levels based on the roles of each user that are based on each client hierarchy structure, work groups, and roles that can be set at different restrictive levels.

Security is provided at the system, server, folder, and application level and is maintained by our IT department. All data transfers require secure FTP login, encryption, or key tags for appropriate transfer. For any other entities to access data in any way, a Business Associate Agreement is required.

Encryption controls include SSL/TLS for web applications and APIs, WPA2 Enterprise for Wi-Fi communications, IPsec for VPN tunnels, and SFTP for secure file transfers. Every client connection is secured by 128 bit SSL encryption via HTTPS and protected by SSL via the web servers.

MC-Rx also uses hardware and software filters that block any non-secure connections between client devices and web applications. All data transfers require secure FTP login, encryption, or key tags for appropriate transfer.

Specific security policies and procedures can be provided upon request.

Unified Group Services Policy

Unified Group Services (Unified) has policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

Procedure

1. All hardware that contains ePHI will remain secured in Unified's offices that are not readily accessible to the public. Such offices will be locked during and outside of business hours. Entry must be granted by an employee of Unified. The security system will be activated when the premises is vacated.
2. All hardware and devices containing ePHI that can be stored in locked storage within the office (such as laptops or other non-desktop devices) will be stored in secure locked storage in the Unified's offices with access limited to only authorized personnel.
3. Employees will be granted physical access to the office as needed to perform their jobs. Each employee will be provided with a building security code and FOB to access the office outside of regular business hours if needed. Employees must take reasonable measures to prevent and detect unauthorized access or damage to the office to protect Unified's information systems. Contract and temporary labor will only gain physical access as required by their job responsibilities as overseen by the manager and permitted by Unified's HIPAA Security Officer.
4. All doors are locked and only authorized visitors are allowed in.
5. All visitors will be required to sign in electronically with a photo ID tag generated. Visitors in areas beyond the reception area or adjacent meeting rooms must be escorted by an employee to prevent such visitors from having any access to ePHI. Upon exiting, visitors must scan their photo ID tag to log their exit.
6. All servers that contain ePHI will be locked in the server room. Access to this room will be restricted to select workforce members, and the room will be kept locked at all times.
7. In the event of a catastrophic data loss, the Security Officer will work with external consultants to procure new equipment and restore data from off-site archived backups. The Security Officer will supervise physical access to the server room.

8. In the event that any individual other than a member of Unified's workforce must have access to software programs for testing and revision, or other systems or access that might include access to PHI, the Security Officer must review and approve of such access and document such access as well as obtain a Business Associate Agreement in accordance with the Unified's Policy.

Describe the data center operational practices.

MC-Rx operates two parallel data centers as mentioned above for real-time replication; one in Gainesville, GA and the other in Lawrenceville, GA. Each data center supports approximately half of the production workload 24/7/365, allowing for load balancing. Each data center has sufficient capacity to support the full production workload with significant expansion capabilities. The two data centers are connected by a primary and secondary link. Data is backed up and copied between the data centers during scheduled daily operations, and each data center contains multiple telecom links to process all online claims. Telecommunications is supplied to each data center with provider diversity from two telecommunications providers at minimum. Secure switching networks have automatic fail over. In summary, each data center has all the capacity and capabilities needed to support the entire production workload.

Describe the physical controls used to secure office facilities that retain hard copy records.

MC-Rx - The facility is protected by electronic access control 24/7. All entrances are under video surveillance 24/7 with access provided to employees through the use of a fob. Fobs can be programmed so that employees can only access the facilities at times specified by management. Data center access is restricted to necessary personnel and is protected by access control with 24/7 video surveillance.

Visitors must have an employee escort while on premises. A visitor log is signed and the records are maintained for 1 year. They are required to present a Government Issued ID to obtain access to the premises and then wear a visitor badge during the duration of their stay.

<u>Unified Group Services Policy</u>
Unified Group Services (Unified) has policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
<u>Procedure</u>

1. All hardware that contains ePHI will remain secured in Unified's offices that are not readily accessible to the public. Such offices will be locked during and outside of business hours. Entry must be granted by an employee of Unified. The security system will be activated when the premises is vacated.
2. All hardware and devices containing ePHI that can be stored in locked storage within the office (such as laptops or other non-desktop devices) will be stored in secure locked storage in the Unified's offices with access limited to only

authorized personnel.

3. Employees will be granted physical access to the office as needed to perform their jobs. Each employee will be provided with a building security code and FOB to access the office outside of regular business hours if needed. Employees must take reasonable measures to prevent and detect unauthorized access or damage to the office to protect Unified's information systems. Contract and temporary labor will only gain physical access as required by their job responsibilities as overseen by the manager and permitted by Unified's HIPAA Security Officer.
4. All doors are locked and only authorized visitors are allowed in.
5. All visitors will be required to sign in electronically with a photo ID tag generated. Visitors in areas beyond the reception area or adjacent meeting rooms must be escorted by an employee to prevent such visitors from having any access to ePHI. Upon exiting, visitors must scan their photo ID tag to log their exit.
6. All servers that contain ePHI will be locked in the server room. Access to this room will be restricted to select workforce members, and the room will be kept locked at all times.
7. In the event of a catastrophic data loss, the Security Officer will work with external consultants to procure new equipment and restore data from off-site archived backups. The Security Officer will supervise physical access to the server room.
8. In the event that any individual other than a member of Unified's workforce must have access to software programs for testing and revision, or other systems or access that might include access to PHI, the Security Officer must review and approve of such access and document such access as well as obtain a Business Associate Agreement in accordance with the Unified's Policy.
9. All repairs and modifications to the physical components of the facilities which are related to security (for example, hardware, walls, doors, and locks) shall be documented. The Security Officer shall maintain such documentation for at least seven (7) years.

Are you able to demonstrate compliance with the HIPAA security and privacy rules?

Yes. MC-Rx maintains strict compliance with HIPAA privacy and security rules. As evidenced throughout our Standard Operating Procedures, we routinely train, test, and discuss the importance of HIPAA, PHI, and privacy compliance with our staff.

There have been no HIPAA violations alleged against MC-Rx in the last 24 months. As with any company that deals with PHI and PII on a minute by minute basis, we have had a limited number of HIPAA release breaches by personnel, all of which have been remediated and resolved, with additional procedures and system changes put in place as needed. MC-Rx has very specific HIPAA policies and procedures, all of which were scrutinized during our recent URAC accreditation and approval process.

Unified has an in-depth HIPAA policy & procedures addressing processes in place to adhere to the HIPAA security and privacy rules. Many of those policy details have been utilized in the technical proposal responses as applicable. We have continual quarterly training and education to maintain high levels of compliance.

Have you completed a security assessment or audit conducted within the last three years? Are you willing to share the results of that assessment/audit?

Yes. Our claims system, security, and regulatory mandates are audited annually, and we are NIST 800-53, SOC1, and URAC certified. We are also in process of obtaining a SOC2 assessment. Yes, we are willing to share the results.

Yes, Unified has had a SOC 1 Type 2 report completed ending 8/31/2020. We are willing to share the results of this audit.

2.4.14 Grievance process

Describe clients and pharmacies are made aware of the grievance process and given access to the forms. This must include Contractor's grievance forms being available upon request on the phone or by direct mail and provides additional methods to complete a grievance.

MC-Rx - Pharmacies are provided information about the grievance process in the online Pharmacy Manual or by calling the Customer Care Center.

Our Customer Care Center documents all calls, complaints, and/or grievances handled by the CSR during the call, and they are escalated to a supervisor for reporting and review for further resolution, as needed.

The reviewing supervisor will document complaints and grievances in the complaint/grievance log. The Customer Care Center also has ticketing reporting capabilities to pull reports by call category, i.e. complaint or grievance.

Every written complaint is acknowledged within two (2) business days; all written complaints are responded to in writing within thirty (30) days.

Unified Group Services – Each EOB that is sent out to providers & clients includes rights to claims review. This outlines the time period for submission as well as where to send the information for the review. Included with the submission is a sample EOB with the claims review language.

Describe how clients and pharmacies access and submit the grievance documents that includes email, direct mail, and any other methods.

For grievances, clients and pharmacies are directed to contact the Customer Care Center. The Customer Care Center will create a trackable ticket for the call and will provide the grievance documents to the caller. The completed documents can be returned by mail, email, or fax.

2.4.15 Implementation components

Define the requirements for implementation of the contract by the go-live date.

As the current administrator for the IDOH HIV Programs, Unified Group Services in conjunction with MC-Rx & Encore Health Network are fully integrated to continue with business operations for these programs. No implementation work is necessary.

Describe how information will be shared and distributed with authorized users prior to the go-live date.

Not Applicable

Describe how the Contactor will work with authorized users to ensure they can access and deliver to IDOH data during the life of the Agreement.

Unified Group Services will continue to work with the team at IDOH to provide any modifications to the allowed benefit coverages, reporting needs, or user access on an as-needed basis. We are here to support your team in maximizing the goals of the programs we administer. We are available at any time to come meet with IDOH staff at their office or we can host the IDOH staff at our offices in Anderson, Indiana.