REMOTE SYSTEM ADMINISTRATION SERVICES

- Statement of Work –

Proprietary and Confidential

rl solutions software for safer healthcare

CONTENTS

1 INTRODUCTION

RL Solutions (RL) has prepared the following Statement of Work (SOW) to provide details on the scope of work associated with Remote System Administration (RSA) services purchased by the Client.

This SOW is not a legal document; it does not supersede any license agreements or other signed agreements between RL Solutions and the Client. The intent of this document is to outline the specific tasks that will be performed by RL Solutions' representative(s) within the scope of the RSA service. If a task is not listed in this document, then the task is not considered within scope of the RSA service.

This SOW is intended solely for Client and RL Solutions only. As such, it cannot be distributed to anyone who is not directly involved without express written consent of both parties.

2 RSA SERVICE HOURS

The RSA hours listed on the Order Form represent the maximum amount of time that RL Solutions resources will provide as part of Remote System Administration services within a one-year period. If a Client has used all annual RSA hours before the end of a given year, the Client may purchase additional hours at the rate outlined on the Order Form.

RL Solutions will track all time spent by all RL Solutions resources on RSA. Activities tracked include, but are not limited to:

- All remote and onsite meetings and conference
- Communications by phone or email
- Technical and non-technical assistance
- Configuration activities
- Internal RL meetings related to the provision of RSA services to the Client
- Preparation of notes/minutes/documentation, etc.

RL Solutions will provide regular quarterly updates on RSA hour use. RL Solutions will also inform the Client when utilization is approaching 50% and 75%. At that time, RL Solutions may also make a recommendation for the best use of the remaining hours and/or the purchase of additional service hours.

Unused service hours expire at the end of the one-year term and cannot be transferred to subsequent years or to other services.

3 SCOPE OF SERVICES

The following section details the specific tasks that will be performed by the RL Solutions Remote System Administrator. The tasks are organized by common features of the product.

3.1 Forms

- Review and maintain current forms (e.g., adding/modifying fields and pick lists and general form layout and behavior).
- Provide suggestions for modification of forms based on recommended best practices, and implementation of changes, if approved by the Client.
    - Creation of new forms including ongoing review and maintenance of those forms that have been approved by the Client.

3.2 Alerts

- Review and maintain current alerts.
- Provide suggestions for modification of alerts based on recommended best practices, and implementation of changes, if approved by the Client.
- Creation of new alerts, including setup of alert definitions, assignment and scheduling that the Client has approved.

3.3 Reports

- Review and maintain corporate level reports and common report templates to be used across all entities, as defined by the Client.
- Provide suggestions for modification of corporate report templates based on recommended best practices, and implementation of changes, if approved by the Client.
- Creation of new corporate level reports, including setup of report templates and scheduling that the Client has approved.
- Setup and maintenance of folder structure for saving of reports at corporate and local levels.

3.4 Schedules

- Guidance on creation and maintenance of schedules for reports and alerts.
- Provide suggestions for modification of schedules based on recommended best practices, and implementation of changes, if approved by the Client.

3.5 User Management

- Guidance to local Client System Administrator on creation and maintenance of user profiles. Assistance, when needed, for more complicated user profiles and scopes.
- Provide suggestions for modification of roles and scopes.

3.6 Security Settings & General System Parameters

- Review application-based security settings contained in the Admin module and general system parameters and suggest changes based on best practices.
- Adjust application-based security settings contained in the admin module and general system parameters as needed.

3.7 File Interchange Module (FIM) for Submission to a Third Party

- Assistance with data mapping and set up of FIM to submit to a third party, in accordance with purchase order for new/additional FIM connector.
- Consultation with contacts at individual entities and a third party to manage the FIM submission process for existing extracts/submissions (e.g., assist with changes to mapping based on permitted modifications to taxonomy).
- Monitoring and troubleshooting of any issues and/or error messages related to FIM submission.

3.8 Upgrades

- Coordinate scheduling, installation, RL testing and rollover to Production for annual and required interim upgrades.
- Group orientation training for key Client resources on upgrade features so that Client can roll out training to end users using a Train-the-Trainer model.

3.9 Training

- Remote group-based new feature training for key Client resources related to an upgrade so that Client can roll out training to end users using a Train-the-Trainer model.
- Client participation in any remote group training sessions offered on occasion by RL Solutions to enhance Client understanding of the software and/or educational offerings made available by RL Solutions via the RL Support Center.
- Other training as required by the Client.

3.10 Requests for Assistance, Investigation of Issues & Troubleshooting

- Creation of tickets for requests/issues directly identified by RSA.

- Overall monitoring of all tickets in the RL Support Center.
- Coordination of RL resources to respond to requests/issues.

3.11 Other Scope Inclusions

RL Solutions will perform the following additional tasks under RSA:

1. Monthly consultation meetings with Client representatives on system utilization and optimization, including an update on all RSA activities performed since last meeting.
2. Continuous monitoring of system utilization and performance to evaluate system optimization and make recommendations for changes/enhancements.
3. Industry and regulatory body requirement guidance to help Client conform to specific requirements and enhance the use of the system (e.g., modifications to stay current with third-party reporting requirements).
4. Manual system environment synchronization of Training and Production databases up to four times per year based on a mutually agreed upon schedule.
5. Manual system environment synchronization of Test database with Production database for purposes on-boarding new sites and/or upgrades.
6. Other projects deemed suitable under the RSA agreement.

3.12 Scope Exclusions

The following section details the specific tasks that are not within the scope of duties performed by the Remote System Administrator.

1. Modification to any forms or the behavior of forms that is not native to the application. In this instance, the Client may submit a product enhancement request to the RL Product Management team for consideration.
2. Creation of issue/enhancement cases for items directly identified by the Client or its representatives. Key Client contacts will be able to submit cases directly to RL via the RL HUB.
3. Coding changes to the software to modify the standard features/functionality of the software.
4. Creation, scheduling, distribution or support of any reports outside of RL6 application (e.g., Excel reports, other third-party reporting tools).
5. Legacy data conversion from historical systems.
6. Implementation services related to the purchase of new products, services and/or licenses.
7. Development and/or technical services related to coding or scripting to change behavior of the software.
8. Development of custom scripts.
9. Database backups or replications, in full or in part, by RL Solutions.
10. Arranging direct database connectivity for Client to access SQL database.
11. Customized SQL queries and associated data extraction.

4 RESPONSIBILITIES OF CLIENT

The following section outlines the responsibilities of the Client in relation to the RSA services.

4.1 Client System Administrator(s)

1. Defining an internal process for oversight, review and approval of requests from all local levels before submitting the request to the RSA.
2. Designation of up to 2 key contacts who will interact with the RSA on a regular basis. These are Client resources familiar with system administration and who are responsible for providing approved direction on system-wide configuration requests related to all sites. This will ensure central coordination of the Client activities, and facilitate concise communication between the Client and the RSA once decisions have been made by the Client.
3. Compliance by all Client key contacts to the process for submitting requests to RSA using RL HUB.
4. Maintenance of applicable corporate and site-level change control records including details related to nature of request, who made request, why request is necessary, and when request was implemented. This information will supplement the details contained in the RL case used by the RSA to document actions taken by RL Solutions.
5. Coordination of Client resources for testing changes related to RSA requests and/or upgrades.
6. Client end user testing of upgrade for sign off prior to rollover into Production environment.
7. Participation in testing of RL6 to sign off on locally requested changes made by the RSA.
8. Participation in testing of RL6 to sign off on upgrade prior to deployment.
9. Participation of key Client resources in any training offered by RL Solutions related to software features/functionality and/or upgrades.
10. Local training of end users to introduce new features and functionality. RL will provide training to key Client resources who can then roll out the training using a Train-the-Trainer model.
11. Sign up to RL'HUB and Connections for online access to cases, knowledgebase and documentation.
12. Physical queuing and sending of files/data to a third party using File Interchange Module. Client will be trained on how to send their data to a third party using FIM.
13. Creation of Level 1 Client Help Desk for local assistance to end users at the local level (e.g., to troubleshoot login issues involving Active Directory, local email issues, email discrepancies, etc.)
14. Investigation and troubleshooting of user login issues related to Client ADT system outside of the interface with RL6. Client IT will be expected to investigate issues related to ADT, local network, etc.
15. Creation of internal Help Desk tickets logged with Client's IT department.
16. Diagnosis/troubleshooting of workstation performance issues that would normally be handled by the Client's IT department.

17. Installing of desktop support components (e.g., Active X, Report Designer component, etc.) that would normally be handled by the Client's IT.
18. Investigation and resolution of Level 1 issues related to matters within jurisdiction of Client Help Desk/IT (e.g., user authentication against Active Directory, email issues outside of RL6, etc.).
19. Resolution of Client Help Desk tickets submitted by Client users. If issues cannot be resolved quickly at a local level, these will be passed on to the RL Solutions Support Team. The Remote System Administrator may be involved in troubleshooting, and the Remote System Administrator may need to submit a case via RL HUB.

5 PROCESS FOR SUBMITTING A REQUEST TO RSA

The following is a detailed explanation of the process for making a request to the RSA.

1. Request is identified at the local level following Client's internal process, and conveyed to the local System Administrator/key Client contact.
2. Designated Client oversight committee will review the proposed request and determine whether to submit the request to the RSA. This is mandatory for any changes to the configuration settings and system parameters. RSA may also be consulted at this time to provide advice/direction on the request before it is submitted to RL Solutions. If request is out of scope and/or if costs are associated with the change, then RL will advise and communicate requirements to Client for consideration.
3. Client approved requests will be submitted to RL Solutions via the RL HUB. RSA will confirm receipt of case and update case with action plan/timeline for response where response will be outside of normal RSA service level agreement.
4. The Client can check the status of case(s) at any time by accessing RL HUB and reviewing cases.
5. All subsequent communication/clarification regarding the initial request will be documented through the RL HUB case. This will ensure there is an accurate record of the request and all actions taken through to closure.
6. Once RSA has completed request, the case will be updated and closed at which time an email notification will be sent to the original submitter. Client key contacts will be able to view all cases via the RL HUB.

6 ASSUMPTIONS

To fulfill the responsibilities of the RSA services, several key assumptions have been made. Any deviations may impact the ability of RL Solutions to provide such services.

6.1 General

1. RSA services shall only extend to the named entities as per the original Order Form.
2. RSA services shall only extend to named products as per the original Order Form. In the event that additional products are purchased subsequent to the RSA agreement, the RSA services will be reviewed and adjustments to the annual service fee will be required.
3. The Client will provide sufficient detail when submitting a request to ensure RSA is able to respond in a timely manner. Insufficient detail will result in an impact to the SLA.
4. More complicated requests (e.g., development of a new form, creation of a complex report) will be handled through a separate agreed upon timeline specific to the request as negotiated by the Client and the RSA.
5. Issues and requests from the Client will be communicated to RL Solutions and the RSA through the RL Support Center ticketing system.
6. Requests from the Client to the RSA will be communicated only by designated Client personnel.

6.2 Technical

1. RL Solutions will be provided with access (including VPN access) to all of the necessary software, systems and servers to perform its responsibilities as part of RSA.
2. Access will be granted in accordance with the RSA Technical Requirements outlined in Section 6 of this this SOW.
3. Issues referred to the RL Solutions Support Team for Level 2 support will be resolved as per the SLA outlined in the RL Solutions Annual Software and Support Maintenance document (www.rlsolutions.com/termsofuse).
4. If applicable, issues related to the hosting of the applications will be addressed by the RL Solution IT team as per the SLA outlined in the RL Solutions Hosting Agreement (www.rlsolutions.com/termsofuse).

7 TECHNICAL REQUIREMENTS FOR RSA

In order to facilitate Remote System Administration services, several technical requirements must be met. These technical requirements ensure appropriate levels of connectivity, access and support to ensure the RSA expert can manage system changes and configurations in an efficient and effective manner. The technical requirements include the following.

7.1 Dedicated environment

- RL Solutions application software must be hosted from a dedicated environment. Software should not be placed/installed on servers for shared purposes.
- Databases may be housed and served from a shared database server, as long as RL Solutions software has dedicated user credentials with Database Owner (DBO) privileges.
- The environment may have network administration tools such as diagnostics and/or server configuration tools, so long as they do not interfere with RL Solutions software.

- Antivirus software is required; however, RL Solutions software and associated network communications are whitelisted.

7.2 Access to the organization

- The Client will provide *Mobile-user VPN* (MUVPN) access to the organization.
- If VPN software is required, a software package must be made available to the RL Solutions team.
- Access security policies, including encryption type and strength will be governed by the Client IT team.
- A dedicated VPN userid/password for RSA. Ideally, this userid/password combination would not expire or can be reset/re-enabled by the RSA expert.
- MUVPN may be implemented using thick client or clientless VPN technologies.
- MUVPN technology used must be IPsec, SSL VPN, L2TP, L2TP over IPSec or SSTP.
- Encryption must comply with DES, 3DES, AES or Diffe-Hellman algorithms and employ a hashing algorithm of MD5 or SHA-1.
- Encryption key strength (i.e. size) must be a minimum 128 bit.
- Authentication password strength to be dictated by the Client's best practices.

7.3 Access to the software environments

7.3.1 For Risk MonitorPro®, Feedback MonitorPro® or Claims MonitorPro®

- Clients will provide access to Thick-client applications, including Report Producer, Administration Client and Web Configuration files. In most instances, the easiest approach is to provision Remote Desktop access to the PRODUCTION server environment. Alternatively, Clients may provision a server or workstation environment with Thick-client applications to negate the need for Remote Desktop access to the PRODUCTION server.
- Appropriate levels of Windows and NTFS folder privileges must be provisioned to be able to modify the web.config and application .ini files in TEST, TRAINING and PRODUCTION environments.
- Clients will provide Remote Desktop access to TEST and TRAINING server environments.
- Clients will provide local administration privileges in the TEST and TRAINING server environments.
- Appropriate levels of RMPro/FMPro/CMPro software privileges must be provisioned to able to facilitate changes within the application.
- Remote Desktop access will be provisioned with Transport Layer Security (TLS) with a minimum 128 bit encryption.
- Remote Desktop connectivity may be provisioned using native Microsoft Windows Terminal Services or other alternative delivery mechanisms, so long as the appropriate client software is provisioned to RL Solutions.

7.3.2 For RL6:Risk, RL6:Feedback, or RL6:Claims

- Clients will provide HTTPS access to the RL6 application. In cases where HTTPS cannot be accommodated, RL6 Clients will provide Remote Desktop access to PRODUCTION server environment. This will avoid any leakage of application layer data including, user credentials.
- Clients will provide Remote Desktop access to TEST and TRAINING server environments.
- Clients will provide local administration privileges in the TEST and TRAINING server environments.
- Clients will provide administrative access to the RL6 software.

7.4 Anti-virus on any server/workstation

Clients will ensure any environment the Remote System Administrator accesses is equipped with anti-virus software and the latest malware/virus definitions are installed.

7.5 Audit changes made to the Windows server

Clients will provision mechanisms to audit access and file changes to the any Windows server environment the Remote Administration System Expert has Remote Desktop privileges to. This will ensure comfort, to both RL Solutions and the Client, that changes are transparent.

7.6 Backup mechanisms

Clients will provide either:

- on-demand access to a DBA resource to facilitate ad-hoc database backups for software environments, prior to changes being made, or
- the necessary SQL tools and storage to facilitate the Remote System Administrator to provision environment backups as required.

7.7 Technical Scope of the RSA

For the duration of the RSA services contract, there will be aspects of the overall environment that will are outside of the scope of RSA work. The RSA is provisioned to deliver application settings and configurations within the scope of the RL6 framework but not beyond. Client IT resources are required to provide troubleshooting and diagnostics assistance for environmental issues, challenges, investigations and/or configurations beyond the boundaries of the RL6 application framework.

In cases where the software is physically hosted with RL Solutions, most IT resource involvement will be offloaded to the RL Solutions IT team. However, Client IT resources will still be required where the application is integrated with internal Client systems, such as LDAP or SMTP.

7.8 IT Resource Involvement

A contact person in IT (IM, IS, etc.) should be identified who will be the Technical Representative and IT Lead for the RL Solutions software. Primary responsibilities of the IT Lead are to coordinate activities for all IT resources for tasks related to the RSA effort and to ensure those resources are made available to complete necessary tasks and provide assistance to the RSA on a timely basis.

The Client is still expected to have an established internal help desk/mechanism for troubleshooting technical issues and Level 1 support issues with end users prior to contacting the RL Solutions Support Team.

IT resources that may *potentially* be required for support include:

- **Firewall administrator** – provide the necessary troubleshooting/diagnostic support for any connectivity or VPN environment issues. This includes working with desktop, server and network teams to resolve performance issues.
- **Network administrator** – provide the necessary troubleshooting/diagnostic support for any connectivity issues. This includes working with desktop, server and firewall teams to resolve performance issues.
- **Server engineer** – ensure installation and configuration of the base software (including database) is complete. Ensure ADT interfaces are feeding the RL Solutions software (if purchased). Ensure SMTP transactions are being sent to the email server. Ensure any additional purchased components are all complete and functional. Support hardware and conduct server maintenance according to Client policy (e.g. apply service packs and other system updates).
- **Software engineer** – Software maintenance, including upgrading RL Solutions software upon a new release.
- **ADT/HL7 administrator** – if HL7 interface purchased, ensure ADT/HL7 data is being sent to the RL Solutions software. Provide the necessary troubleshooting/diagnostic support for any issues surrounding the ADT/HL7 feed(s).
- **Email administrator** – ensure the RL Solutions software is permitted to send SMTP/email through the Client email server environment. Provide the necessary troubleshooting/diagnostic support for email related issues.
- **Database administrator** – ensure regular database backups are being executed and verified. Facilitate ad-hoc database backups for software environments, prior to changes being made. Provide the necessary troubleshooting/diagnostic support for database related issues. This includes working with desktop, server and firewall teams to resolve performance issues.
- **Desktop engineer** – where necessary, thick client applications are installed appropriately. Ensure sufficient levels of desktop privileges, such as NTFS/folder privileges, are configured to administer the RL Solutions software.
- **Technical support** – ensure user profiles and thick client applications are functioning as expected and facilitate support where required.

8 SERVICE LEVEL AGREEMENT

Access to RSA services is available Monday to Friday from 8:30am to 5:30pm Eastern Time.

RL Solutions will strive to complete requests made within the scope of RSA services within 3 business days of receipt of sufficient details.

Any requests that are deemed to be more complex in nature, such as custom forms design or custom report design, may be treated as special projects, and a mutually agreed upon timeline for completion will be determined by the Client and RSA.