<p align="center">**Exhibit to Cloud Services Agreement:**</p>

<p align="center">**Service Level Agreement**</p>

<p align="center">**All information, including pricing, contained in this Exhibit is confidential.**</p>

This Exhibit sets forth the applicable Service Levels, which includes the Service Levels Objective of the Cloud Service, and the associated Support Services.

1.   DEFINITIONS

Unless otherwise noted the definitions in this Exhibit shall have the same meaning as set forth in the Agreement.

"Business Day" means Monday to Friday, excluding public holidays in the Support Region.

"**Corrective Action Plan**" has the meaning as described under Section 4.1(viii) of this Exhibit.

"**Downtime**" is anytime where the Cloud Services are not substantially available for use by the Customer, other than Downtime Exclusions.

"**Downtime Exclusions**". Downtime does not include unavailability caused by: (1) Scheduled Maintenance or a suspension of Cloud Services; (2) flaws in Customer's Data; (3) the incompatibility of any operating system, Interfaced Applications or vendor supplied security patches with Customer's Data or the Software; (4) acts or omissions of Customer or its agents, including all testing of the servers by Customer or a third party vendor; (5) the failure of servers or services outside of a Datacenter on which the Cloud Services are dependent, including, but not limited to, inaccessibility on the Internet that is not caused by Company's network or network providers, or failure of VPN connectivity caused wholly or in part by systems not managed by Company as part of the Cloud Service; (6) Company's blocking of Customer Data that Company deems in its sole reasonable discretion to be in violation of applicable laws (including HIPAA) or other health care regulations; (7) a force majeure event as described in the Agreement or events not in Company's direct control; (8) a denial of service attack or unauthorized access (i.e., hacking); (9) Customer's failure to meet the terms and conditions of this Agreement, including but not limited to its failure to install and implement the latest Update that Company makes available; (10) Customer's configuration or use of the system in a manner that exceeds the resource capacities of the Cloud Service; and (11) where an upgrade may be expected to significantly interrupt operation of the Cloud Service or require Customer actions to reconfigure routes or other aspects of the Cloud Service or non-Cloud Service systems. Downtime also excludes: (12) Downtime in co-located devices; (13) Downtime not reported by Customer within one Business Day of the day the Downtime first began; (14) time required to format or reformat disks or a RAID array; (15) time required to load, reload, configure or reconfigure an operating system; (16) time required to load, reload, configure or reconfigure Interfaced Applications; (17) time required to restore from backup; (18) unavailability of non-production installations or environments; and (19)) the failure of servers or services not provided by Company on which the Cloud Services are dependent.

"**Fault Level**" or "**Fault**" means the Fault levels specified in the table in section 5 below, in relation to each request for Support Services received by Company's support center from Customer, which shall be mutually agreed by Company and Customer (or failing agreement, as determined by Company). In instances where a reported Fault is determined by Company to be in relation to an enhancement then Company reserves the right to lower the Fault Level.

"**Initial Response Time**" means the elapsed time between when Company receives notification of a request for Support Services by Customer and the time that Company acknowledges receipt of that request.

"Monthly Cloud Service Fees" means 1/12 times the annual Subscription Fees amount defined in the Initial Schedule of this agreement.

"Normal Business Hours" means, depending on the Support Region: 07:00 to 16:00 Philippines time (for the Asia/Pacific region); 08:00 to 17:00 GMT/BST (for the Europe, Middle East, and Africa region); and 09:00 to 18:00 EST/EDT (for the North America region).

"**Progress Report**" means the update provided by Company to Customer by phone or email in respect of resolution of each request for Support Services submitted by Customer.

"**Scheduled Maintenance**" means periodic scheduled upgrades and maintenance on the Cloud Service and supporting Software, which will require making the Cloud Service unavailable for limited times. Examples of downtime for scheduled maintenance may include upgrades to hardware, network device operating systems or configurations, application server operating systems, upgrades or configuration changes to hosted applications, upgrades or configuration changes to database software and upgrades or configuration changes to virtual software management systems.

"**Support Region**" has the meaning of the (i) United Kingdom (for Europe, Middle East, and Africa), (ii) Philippines (for the East Asia/Pacific region), or (iii) the United States East Coast (for North America). Customer shall select one of the three regions set forth in the preceding sentence upon the Agreement's Effective Date as the basis for Support Services going forward.

"**Support Services**" has the meaning described in Section 4 "Support Services" in this Exhibit.

"**Target Resolution Time**" means the target elapsed time between when Company receives notification of a request for Support Services by Customer and the time a final position is agreed between Company and Customer, where either a solution (which may be remedying the Fault or providing a work-around) has been reached or no further action can be taken under the terms of this Agreement. This time is a target only, and Company does not guarantee that any particular request for Support Services will be resolved within the specified time period. The Target Resolution Time does not include any time spent waiting for a response from Customer.

2.   SERVICE LEVEL

Company will use commercially reasonable efforts to meet the service levels identified below (together, the "**Service Level(s)**"):

     i.   **Data Backup**. If applicable, scheduled backup jobs will be completed every day. A back-up job that initially is unsuccessful, but is subsequently corrected within one Business Day shall be considered a successful backup for these purposes. Measurement of this objective will occur daily. Regular or continuous replication of data to a local data storage device or a remote data center shall meet the data backup requirement.

    ii.   **Target Response and Resolution Time Objectives** (as defined in the section titled Support Services below). Target Response Time Objectives and Target Resolution Time Objectives are set forth in the Table 1 below.

   iii.   **System Availability**. Company will make the Cloud Service available such that the amount of Downtime in a given month will not exceed 0.1%.

3.   LIMITATIONS ON SERVICE LEVELS

The Service Levels will not apply if: (1) Customer disables (either intentionally or unintentionally) Company's administrative access to the configuration (e.g., by changing a password); (2) Customer makes any modifications that prohibit the Cloud Services from working properly; (3) Customer modifies or deletes the contents of Company's administrative directories, or disables or modifies any software installed by Company for the purposes of monitoring or server maintenance; (4) Customer violates the terms of this Agreement; (5) Customer becomes ineligible for service credits pursuant to any other provision of this Agreement; or (6) if the error is caused by an Interfaced Application or other, non-Company provided software or system. If Customer engages in one or any combination of the activities specified in this Section 2, Company may perform Additional Services without Customer's prior approval, which Customer will be required to pay for in accordance with the fee schedule set forth herein.

4.   SUPPORT SERVICES

4.1 During the Initial Term and any renewal term, Company shall provide the support services for the Cloud Service as described below and in the Documentation (the "**Support Services**"). Company shall:

    iv.   Correct any failure of the Cloud Services to perform substantially in accordance with the specifications of the Cloud Services or any Software contained therein, including without limitation, defect repair, programming corrections, and remedial programming or a procedure or routine that, when observed in regular operation of the Cloud Service, eliminates the practical adverse effect of the Fault.

    v.   Provide all updates, bug fixes, enhancements, new releases and version, and other improvements to the Cloud Services that Company provides to its other similarly situated customers at no additional charge.

    vi.   Provide unlimited access for up to five (5) named users to the support ticketing system to log any issue. Telephone support is during Normal Business Hours or Business Days in the applicable Support Region, unless otherwise specified herein.

   vii.   Provide online access to technical support bulletins and other user support information and forums; to the extent Company makes such resources available to its customers.

  viii.   In the event that a Fault Level 1 Incident occurs, Company shall promptly investigate the root causes of such support issues and shall provide to Customer within ten (10) days of the occurrence of the Fault Level 1 Incident an analysis of such root causes and a proposed corrective action plan for Customer's review, comment and approval (the "**Corrective Action Plan**"). The Corrective Action Plan shall include, at a minimum: (i) a commitment by Company to Customer to devote the appropriate time, skilled personnel, systems support and equipment, and/or resources to remedy the Fault Level 1 incident; (ii) a strategy for developing any programming/software updates, fixes, patches, etc. necessary to remedy, and prevent any further occurrences of such incidents; and (iii) time frames

for implementation of the Corrective Action Plan. There shall be no additional charge (other than those fees set forth in this Agreement) for Customer's implementation of such Corrective Action Plan in the time frames and manner set forth in the Corrective Action Plan. Company will not be responsible for any cost that the Customer may incur in making changes to resolve Fault Level 1 incidents.

4.2   Customer's support staff will be responsible for first-level support, including (without limitation) the provision of an internal support desk service to end users of the Cloud Service for providing general assistance and initially diagnosing any operational or functional problems with the Cloud Service. Customer's support staff shall timely report Faults that cannot be solved internally in accordance with the procedure outlined in the Support Manual. Support requests may be logged by Customer in relation to the use of the Cloud Service in a non-production environment, provided that such calls are not subject to the Support Service response targets set forth in Section 5 below. To the extent that a Fault is caused by Interfaced Applications, Company will use reasonable efforts to resolve such Fault through recourse to the third party licensor, but such Faults shall not be subject to the Support Service response targets set forth in Section 5 below.

4.3   Customer shall ensure that its support staff are familiar with and knowledgeable about the functional capabilities and technical operation of the Cloud Service. If they are not available or are unable to attend within a reasonable time period in relation to a response by Company to a support request, Company reserves the right to lower the Fault Level.

4.4   No back-end access to any Company environments will be provided to the Customer. Additional environments will need to be set up for Customer testing purposes at an additional cost following a detailed review of additional requirements.

4.5   Company may charge Customer in accordance with the Professional Services Rates, as defined in the Initial Schedule, for any support outside the scope of the Support Services, including first-level support requests for assistance with respect to use of the Cloud Service or other matters not relating to Faults (e.g., troubleshooting for problems not relating to Faults).

4.6   Company routinely modifies and enhances the Cloud Service for the purpose of correcting errors, and to make available new releases and new versions of the Cloud Service. While Customer subscribes to the Cloud Service and provided Customer is not in breach of its obligations under this Agreement, Company will make Updates available to Customer electronically. Customer agrees to maintain both an email address, and a method and means to download Updates from Company. Company will use this email address to notify Customer regarding Updates to the Software. Customer agrees to promptly install Updates to maintain the Cloud Service at the most current level.

4.7   Customer acknowledges that Company provides Support Services remotely from Company's offices in the United States, United Kingdom, Australia, Philippines, United Arab Emirates, New Zealand, and at other locations chosen exclusively by Company. Customer acknowledges that the provision of Company Support and other services will necessitate the transfer of data by Company to, and the processing of that data by, its staff in those offices, and Customer hereby consents to Company transferring and processing that data.

5   TARGET INCIDENT RESPONSE AND RESOLUTION TIME

An incident / issue priority can be set with a second set of definitions to include urgency which can be set by the Customer. The Customer can increase the priority of an issue to guide the support team as to which issue to fix first. Customers can therefore set the issue urgency (low / medium / high) to indicate the priority of the issue. Company will only pay service credits based on impact. Company will respond to Faults in accordance with this table below:

Fault Level	Target Initial Response Time	Target Initial Response Time Objectives	Target Resolution Time	Target Resolution Time Objectives	Coverage Hours
Level 1	30 minutes	99%	4 hours	99%	24/7
Level 2	1 hour	99%	8 hours	99%	24/7
Level 3	Next Business Day	95%	2 weeks	None	Normal Business Hours
Level 4	2 Business Days	90%	By arrangement	None	Normal Business Hours

Fault Level	Definitions
Level 1	Critical business impact – means an incident that causes complete loss of Service to Customer's production environment such that work cannot reasonably continue and no workarounds to provide all of the functionality of the Service required under the agreement are possible or cannot be implemented in time to minimize the impact on Customer's business.

Level 2	Significant Business Impact – means an incident that results in a significant loss of service to Customer's production environment such that processing can proceed in a restricted fashion, but performance is significantly reduced and/or operation of the service is considered severely limited and no workaround to provide the affected functionality is possible or cannot be implemented in time to minimize the impact on Customer's business.
Level 3	Minor Business Impact – means an incident that results in minimal loss of service thereof to Customer's production environment such that the impact of the incident is minor or an inconvenience, such as requiring a manual bypass to restore product functionality
Level 4	No Business Impact – means an incident that causes no loss of service and in no way impedes Customer's use of service in accordance with the agreement.

6 SERVICE CREDITS

Customer's sole remedy for Company's failure to achieve the Service Levels set forth in this Exhibit shall be the service credits identified below ("**Service Credits**"). Customer will not be eligible for Service Credits for Downtime, including delays in restoring the Services, resulting from Customer's failure to provide current and accurate contact information.

(i) **Data Backup Agreement**. The penalty for not meeting the requirements set forth in Section 2.i of this Exhibit in any given month will be 1% of the Monthly Cloud Service Fees for such monthly period.

(ii) **Response and Resolution Time**. The penalty for not meeting Level 1 or Level 2 Target Initial Response Time Objectives more than once in any given month will be 2% of the Monthly Cloud Service Fees. The penalty for not meeting Level 1 or Level 2 Target Resolution Time Objectives more than once in any given month will be 2% of the Monthly Cloud Service Fees.

(iii) **Service Credits Calculation**. If the Service Level is less than 99.9%, and if Customer has fulfilled all of its obligations under the Agreement including this Exhibit, Company will provide Customer with a Service Credit applied to that month's Monthly Cloud Service Fees in which the failure to meet this Service Level requirement has occurred. Such a Service Credit will be calculated in accordance with the table below.

% of Cloud Services Availability per Calendar Month	Service Credit
99.5% - 99.89%	2.5%
99.0% - 99.49%	5%
98.0% - 98.99%	10%
97.0% - 97.99%	15%
96.0% - 96.99%	20%
Less than 96.0%	25%

7 SERVICE CREDIT PROCEDURES

The maximum combined amount of all Service Credits earned in a given calendar month may not exceed 25% of the Monthly Cloud Service Fees for the calendar month in which the events giving rise to the Service Credits occurred. Company will apply Service Credits to the invoice immediately following its determination of Service Credit eligibility and amount.

If Customer disputes Company's calculation of Service Level performance or Service Credits, any data used to calculate such values, or any other subject matter of this Exhibit 3, Customer must notify Company, within thirty (30) days after failure to achieve the service levels, in writing of the basis of such dispute, in which case Company shall respond promptly to such notice and the Parties shall use good faith efforts to resolve such dispute in a timely manner. No such claims or any other remedy will be available to Customer after the 30-day period.

8 RESPONSIBILITY MATRIX(S)

8.1 Definitions:
R stands for **"Responsible"** and indicates which party is responsible for the function.
A stands for **"Accountable"**, which denotes which party is approving or accountable for approving the function listed.

C stands for **"Consulted"** which specifies that a party is consulted for their opinion on the function listed.
I stands for **"Informed"** and indicates that a party will be told of progress or decisions made on the function listed.
"**IoP**" means Interoperability Platform
"**EDP**" means edge device platform

8.2 Envoy Managed Services

Activity	Company	Customer
Infrastructure for IoP hosting in cloud environment configured to meet regulatory requirements	R, A	I
Infrastructure for IoP Provisioning (compute, networking, storage)	R, A	I
Infrastructure for IoP Access Controls	R, A	I
Infrastructure for IoP Performance Monitoring (compute, networking, storage)	R, A	I
Infrastructure for IoP Performance Optimization (compute, networking, storage)	R, A	I
Infrastructure for IoP Patch Management	R, A	I
Infrastructure for IoP Monitoring for Malware and Intrusion	R, A	I
Infrastructure for IoP Availability	R, A	I
Encryption of Data at Rest within the IoP	R, A	I
Encryption of Data in motion	Shared	Shared
IoP Provisioning	R, A	I
IoP Monitoring	R, A	I
IoP Configuration Backup	R, A	I
IoP Message Data Backup	C, I	R, A
Deployment of IoP Upgrades and Updates	R, A	C, I
Change control and testing of major IoP upgrades and updates	Shared	Shared
Configuration of Data Exchange Mechanisms between IoP and Customer Systems	Shared	Shared
Configuration of Customer Systems to Enable Data Exchange Mechanisms with IoP	C, I	R, A
Encryption Keys and Renewal (for example, SSL) Used to Send Data to IoP	R, A	C, I
Project Management for Implementation	R, A	C, I
Project Management for new sites and connections	R, A	C, I
Periodic disaster recovery testing	C (additional fees apply)	R, A
Periodic penetration testing of cloud infrastructure and IoP	R, A	C, I
Notification of abnormal/unusual traffic and downtimes under Customer (or End User) control	C, I	R, A

8.3 Rhapsody as a Service/Corepoint as a Service

Activity	Company	Customer
Infrastructure for IoP hosting in cloud environment configured to meet regulatory requirements	R, A	I
Infrastructure for IoP Provisioning (compute, networking, storage)	R, A	I
Infrastructure for IoP Access Controls	R, A	I
Infrastructure for IoP Performance Monitoring (compute, networking, storage)	R, A	I
Infrastructure for IoP Performance Optimization (compute, networking, storage)	R, A	I
Infrastructure for IoP Patch Management	R, A	I
Infrastructure for IoP Monitoring for Malware and Intrusion	R, A	I
Infrastructure for IoP Availability	R, A	I
Encryption of Data at Rest within the IoP	R, A	I
Encryption of Data in motion	Shared	Shared
IoP Provisioning	R, A	I
IoP Monitoring	R, A	I
IoP Configuration Backup	R, A	I
IoP Message Data Backup	C, I	R, A
Deployment of IoP Upgrades and Updates	R, A	C, I
Change control and testing of major IOP upgrades and updates	Shared	Shared
Configuration of Data Exchange Mechanisms between IoP and Customer Systems	Shared	Shared
Configuration of Customer Systems to Enable Data Exchange Mechanisms with IoP	-	R, A
Interface Development	-	R, A

Activity	Company	Customer
Interface Monitoring	-	R, A
Interface Optimization	-	R, A
Interface Troubleshooting	Shared	Shared
Interface data volume monitoring and configuration of data expiration	R, A	C, I
Encryption Keys and Renewal (for example, SSL) Used to Send Data to IoP	R, A	C, I
Project Management for Implementation	C, I	RA
Project Management for new sites and connections	-	RA
Periodic disaster recovery testing	C (additional fees apply)	RA
Periodic penetration testing of cloud infrastructure and IoP	RA	CI
Notification of abnormal/unusual traffic and downtimes under Customer (or End User) control	CI	RA

8.4 API Gateway

Activity	Company	Customer
Infrastructure for IoP hosting in cloud environment configured to meet regulatory requirements	R, A	I, C
Infrastructure for IoP Provisioning (compute, networking, storage)	R, A	I
Infrastructure for IoP Access Controls	R, A	I
Infrastructure for IoP Performance Monitoring (compute, networking, storage)	R, A	I
Infrastructure for IoP Performance Optimization (compute, networking, storage)	R, A	I
Infrastructure for IoP Patch Management	R, A	I
Infrastructure for IoP Monitoring for Malware and Intrusion	R, A	I
Infrastructure for IoP Availability	R, A	I
Encryption of Data at Rest within the IoP	R, A	I
Encryption of Data in motion	Shared	Shared
IoP Provisioning	R, A	I
IoP Monitoring	R, A	I
IoP Configuration Backup	R, A	I
IoP Message Data Backup	R, A	C, I
Deployment of IoP Upgrades and Updates	R, A	C, I
Change control and testing of major IOP upgrades and updates	R, A	I
Configuration of Data Exchange Mechanisms between IoP and Customer Systems	Shared	Shared
Configuration of Customer Systems to Enable Data Exchange Mechanisms with IoP	-	R, A
Gateway Development	Shared	Shared
Gateway Monitoring	-	R, A
Gateway Troubleshooting	Shared	Shared
API call volume monitoring	C, I	R, A
Project Management for Gateway Implementation	C, I	RA
Project Management for new API Gateways	-	RA
Periodic disaster recovery testing	R, A	C, I
Periodic penetration testing of cloud infrastructure and IoP	RA	CI
Notification of abnormal/unusual traffic and downtimes under Customer (or End User) control	CI	RA

8.5 Envoy Managed Services (edge device)
Company will host Envoy Edge Device within a remote container (i.e., a virtual machine). Customer is responsible for maintaining its own hosted environment and must install the Company-provided virtual machine.

Activity	Company	Customer
Infrastructure for EDP hosting in a remote container configured to meet Company-provided specifications	C, I	R, A
Infrastructure for EDP Provisioning (compute, networking, storage)	C, I	R, A
Infrastructure for EDP Access Controls	R, A	C, I
Infrastructure for EDP Performance Monitoring (compute, networking, storage)	C, I	R, A
Infrastructure for EDP Performance Optimization (compute, networking, storage)	C, I	R, A
Infrastructure for EDP Patch Management	R, A	C, I
Infrastructure for EDP Monitoring for Malware and Intrusion	R, A	C, I

Infrastructure for EDP Availability	Shared	Shared
Encryption of Data at Rest within the EDP	R, A	I
Encryption of Data in motion	Shared	Shared
EDP Provisioning	C, I	R, A
EDP Monitoring	R, A	I, C
EDP Configuration Backup	R, A	I
EDP Message Data Backup	C, I	R, A
Deployment of EDP Upgrades and Updates	R, A	C, I
Change control and testing of major EDP upgrades and updates	Shared	Shared
Configuration of Data Exchange Mechanisms between EDP and Customer Systems	Shared	Shared
Configuration of Customer Systems to Enable Data Exchange Mechanisms with EDP	C, I	R, A
Interface Development	R, A	C, I
Interface Monitoring	R, A	C, I
Interface Optimization	R, A	C, I
Interface Troubleshooting	Shared	Shared
Interface data volume monitoring and configuration of data expiration	R, A	C, I
Encryption Keys and Renewal (for example, SSL) Used to Send Data to EDP	R, A	C, I
Project Management for Implementation	R, A	C, I
Project Management for new sites and connections	R, A	C, I
Periodic disaster recovery testing	Shared (additional fees apply)	Shared
Periodic penetration testing of cloud infrastructure and EDP	R, A	C, I
Notification of abnormal/unusual traffic and downtimes under Customer (or End User) control	C, I	R, A

8.6 Rhapsody EMPI

8.6.1 – SaaS EMPI

Activity	Company	Customer
Infrastructure for EMPI provisioning (compute, storage, networking)	R, A	I
Infrastructure for EMPI access controls	R, A	C, I
Infrastructure for EMPI monitoring (availability and security)	R, A	I
Infrastructure security patching and version updates (OS, database)	R, A	I
Encryption of EMPI data at rest and data over the wire	R, A	I
Network configuration, IP whitelisting, to support EMPI connectivity from customer network	C, I	R, A
Solution design and architecture	R, A	C, I
EMPI application installation and configuration	R, A	C, I
Configuration and monitoring of Single Sign On integration	C, I	R, A
Data analysis and EMPI tuning during initial implementation	R, A	C, I
Source system data file extracts to support analysis and initial load	C, I	R, A
Initial data loads prior to go-live	R, A	I
Acceptance testing of EMPI matching and integration	C, I	R, A
Implementation project management	Shared	Shared
Development of interfaces to Integration Engine from connected systems (HL7, batch file, etc.)	C, I	R, A
Development of interfaces to EMPI from Integration Engine through REST web services	C, I	R, A
Development of interfaces to receive notifications (HL7, batch file, etc.) from Integration Engine	C, I	R, A
Development of REST service to receive EMPI notifications in Integration Engine	C, I	R, A
Certificate issuance, monitoring, and renewal for EMPI infrastructure	R, A	I
Certificate issuance, monitoring, and renewal for Customer infrastructure	C, I	R, A
EMPI application monitoring (availability and security)	R, A	I
EMPI application security patches and product patches	R, A	I
EMPI product upgrades (Professional Services engagement for customer hosted)	R, A	I
Change control process	Shared	Shared
Application testing and validation for application changes	C, I	R, A
Application performance monitoring, environment sizing	R, A	I
Application product support	R, A	C, I
Annual disaster recovery testing	R, A	I
Annual security penetration testing	R, A	I
EMPI match quality and data quality monitoring	R, A	I
Regular EMPI data stewardship of potential duplicates/potential matches	I	R, A
Regular EMPI data stewardship of potential overlays	I	R, A
Annual EMPI Healthcheck (included with SaaS EMPI)	R, A	C, I

8.6.2 – SaaS EMPI with Envoy, or Rhapsody PS implemented Integration

Activity	Company	Customer
Infrastructure for EMPI provisioning (compute, storage, networking)	R, A	I
Infrastructure for EMPI access controls	R, A	C, I
Infrastructure for EMPI monitoring (availability and security)	R, A	I
Infrastructure security patching and version updates (OS, database)	R, A	I
Encryption of EMPI data at rest and data over the wire	R, A	I
Network configuration, IP whitelisting, to support EMPI connectivity from customer network	C, I	R, A
Solution design and architecture	R, A	C, I
EMPI application installation and configuration	R, A	C, I
Configuration and monitoring of Single Sign On integration	C, I	R, A
Data analysis and EMPI tuning during initial implementation	R, A	C, I
Source system data file extracts to support analysis and initial load	C, I	R, A
Initial data loads prior to go-live	R, A	I
Acceptance testing of EMPI matching and integration	C, I	R, A
Implementation project management	Shared	Shared
Development of interfaces to Integration Engine from connected systems (HL7, batch file, etc.)	C, I	R, A
Development of interfaces to EMPI from Integration Engine through REST web services	R, A	C, I
Development of interfaces to receive notifications (HL7, batch file, etc.) from Integration Engine	C, I	R, A
Development of REST service to receive EMPI notifications in Integration Engine	R, A	C, I
Certificate issuance, monitoring, and renewal for EMPI infrastructure	R, A	I
Certificate issuance, monitoring, and renewal for Customer infrastructure	C, I	R, A
EMPI application monitoring (availability and security)	R, A	I
EMPI application security patches and product patches	R, A	I
EMPI product upgrades (Professional Services engagement for customer hosted)	R, A	I
Change control process	Shared	Shared
Application testing and validation for application changes	C, I	R, A
Application performance monitoring, environment sizing	R, A	I
Application product support	R, A	C, I
Annual disaster recovery testing	R, A	I
Annual security penetration testing	R, A	I
EMPI match quality and data quality monitoring	R, A	I
Regular EMPI data stewardship of potential duplicates/potential matches	I	R, A
Regular EMPI data stewardship of potential overlays	I	R, A
Annual EMPI Healthcheck (included with SaaS EMPI)	R, A	C, I

8.6.3 – Customer Hosted EMPI, Customer implemented Integration

Activity	Company	Customer
Infrastructure for EMPI provisioning (compute, storage, networking)	C, I	R, A
Infrastructure for EMPI access controls	C, I	R, A
Infrastructure for EMPI monitoring (availability and security)	C, I	R, A
Infrastructure security patching and version updates (OS, database)	C, I	R, A
Encryption of EMPI data at rest and data over the wire	C, I	R, A
Network configuration, IP whitelisting, to support EMPI connectivity from customer network	C, I	R, A
Solution design and architecture	R, A	C, I
EMPI application installation and configuration	R, A	C, I
Configuration and monitoring of Single Sign On integration	C, I	R, A
Data analysis and EMPI tuning during initial implementation	R, A	C, I
Source system data file extracts to support analysis and initial load	C, I	R, A
Initial data loads prior to go-live	R, A	I
Acceptance testing of EMPI matching and integration	C, I	R, A
Implementation project management	Shared	Shared
Development of interfaces to Integration Engine from connected systems (HL7, batch file, etc.)	C, I	R, A
Development of interfaces to EMPI from Integration Engine through REST web services	C, I	R, A
Development of interfaces to receive notifications (HL7, batch file, etc.) from Integration Engine	C, I	R, A
Development of REST service to receive EMPI notifications in Integration Engine	C, I	R, A
Certificate issuance, monitoring, and renewal for EMPI infrastructure	C, I	R, A
Certificate issuance, monitoring, and renewal for Customer infrastructure	C, I	R, A
EMPI application monitoring (availability and security)	C, I	R, A
EMPI application security patches and product patches	C, I	R, A
EMPI product upgrades (Professional Services engagement for customer hosted)	R, A	C, I
Change control process	C, I	R, A
Application testing and validation for application changes	C, I	R, A
Application performance monitoring, environment sizing	C, I	R, A
Application product support	C, I	R, A
Annual disaster recovery testing	C, I	R, A
Annual security penetration testing	C, I	R, A
EMPI match quality and data quality monitoring	C, I	R, A
Regular EMPI data stewardship of potential duplicates/potential matches	I	R, A
Regular EMPI data stewardship of potential overlays	I	R, A
Annual EMPI Healthcheck (included with SaaS EMPI)	N/A	N/A

8.6.4 – Customer Hosted EMPI, Rhapsody PS implemented Integration

Activity	Company	Customer
Infrastructure for EMPI provisioning (compute, storage, networking)	C, I	R, A
Infrastructure for EMPI access controls	C, I	R, A
Infrastructure for EMPI monitoring (availability and security)	C, I	R, A
Infrastructure security patching and version updates (OS, database)	C, I	R, A
Encryption of EMPI data at rest and data over the wire	C, I	R, A
Network configuration, IP whitelisting, to support EMPI connectivity from customer network	C, I	R, A
Solution design and architecture	R, A	C, I
EMPI application installation and configuration	R, A	C, I
Configuration and monitoring of Single Sign On integration	C, I	R, A
Data analysis and EMPI tuning during initial implementation	R, A	C, I
Source system data file extracts to support analysis and initial load	C, I	R, A
Initial data loads prior to go-live	R, A	I
Acceptance testing of EMPI matching and integration	C, I	R, A
Implementation project management	Shared	Shared
Development of interfaces to Integration Engine from connected systems (HL7, batch file, etc.)	C, I	R, A
Development of interfaces to EMPI from Integration Engine through REST web services	R, A	C, I
Development of interfaces to receive notifications (HL7, batch file, etc.) from Integration Engine	C, I	R, A
Development of REST service to receive EMPI notifications in Integration Engine	R, A	C, I
Certificate issuance, monitoring, and renewal for EMPI infrastructure	C, I	R, A
Certificate issuance, monitoring, and renewal for Customer infrastructure	C, I	R, A
EMPI application monitoring (availability and security)	C, I	R, A
EMPI application security patches and product patches	C, I	R, A
EMPI product upgrades (Professional Services engagement for customer hosted)	R, A	C, I
Change control process	C, I	R, A
Application testing and validation for application changes	C, I	R, A
Application performance monitoring, environment sizing	C, I	R, A
Application product support	C, I	R, A
Annual disaster recovery testing	C, I	R, A
Annual security penetration testing	C, I	R, A
EMPI match quality and data quality monitoring	C, I	R, A
Regular EMPI data stewardship of potential duplicates/potential matches	I	R, A
Regular EMPI data stewardship of potential overlays	I	R, A
Annual EMPI Healthcheck (included with SaaS EMPI)	N/A	N/A