

## **Extensions For Healthcare Services Description**

### **1. Services Description**

This services description (“**Services Description**”) applies to UKG’s provision of the Workforce Forecast Manager for Healthcare SaaS, Workforce Workload Manager for Healthcare SaaS, Workforce Target Intelligence for Healthcare SaaS, the Workforce Extensions for Healthcare Bundle, WF Extensions for Healthcare and related services in UKG’s hosting environment (the “**Subscription Services**” or “**Healthcare Extensions**”) when set forth on the Order. Subscription Services shall be delivered by means of Customer’s permitted access to the infrastructure hosting the Subscription Services. This Services Description is subject to and governed by the Order and the corresponding agreement that governs Customer’s use of UKG Workforce Management and other Services (collectively, the “**Agreement**”).

### **2. Definitions**

“**Cloud Services for Healthcare Extensions**” means those services described in **Exhibit 1**, the “Cloud Services for Healthcare Extensions”.

“**Encrypt**” or “**Encryption**” means to cryptographically protect data using methods such as symmetric encryption algorithm, asymmetric encryption algorithm or a one-way hashing algorithm.

“**Encryption Gateway Tool**” means the WF Extensions for Healthcare Encryption Gateway for UKG Cloud tool described in section 5.

“**HIPAA**” means the Health Insurance Portability & Accountability Act of 1996, P.L. 104-191, as amended from time to time, together with its implementing regulations promulgated under HIPAA and under the Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”), Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (“ARRA”), by the U.S. Department of Health and Human Services, including, but not limited to, the Privacy Rule, the Security Rule and the Breach Notification Rule, as amended from time to time.

“**PHI**” means Protected Health Information as defined by HIPAA.

“**Solution**” means the combination and use of the Healthcare Extensions working with the Encryption Gateway Tool.

### **3. Data Security**

As part of the Subscription Services, UKG shall provide those administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer data as described in **Exhibit 2** herein. These terms, as well as the Business Associate Addendum that the parties may enter into, replace any Data Security and Privacy terms outlined in the Master Services Agreement or data protection addendum for the purposes of the Healthcare Extensions.

### **4. UKG Responsibilities**

UKG offers the Service Level Agreement and associated SLA Credits attached hereto and incorporated herein by reference as **Exhibit 3** for the Subscription Services.

### **5. Encryption Gateway**

#### **5.1 Description of the Encryption Gateway Tool**

- (a) As part of Subscription Services, UKG licenses to Customer the right to install and use the WF Extensions for Healthcare Encryption Gateway for UKG Cloud tool (“**Encryption Gateway Tool**”) in accordance with the terms of this Services Description. The Encryption Gateway Tool will Encrypt PHI before it is transmitted to the UKG Cloud and it will un-Encrypt the PHI when it is extracted from the UKG Cloud in accordance with the Encryption Gateway Tool documentation. It shall be Customer’s responsibility to install and apply updates to the Encryption Gateway Tool in accordance with Section 5.2 below.
- (b) UKG will deliver the Encryption Gateway Tool by giving Customer access to the secure Customer portal and such tool shall be available for download and to be installed by Customer, on Customer’s server and behind its firewall at its facility location. The Encryption Gateway Tool will be under the Customer’s control at all times and Customer shall install updates to the Encryption Gateway Tool when such updates are made available by UKG. The Encryption Gateway Tool is licensed to Customer concurrently with the Healthcare Extensions and upon termination or expiration of Subscription Services, Customer’s right to use the Encryption Gateway Tool shall also terminate. Customer agrees to uninstall the Encryption Gateway Tool upon termination of Customer’s right to use the Subscription Services.
- (c) The Encryption Gateway Tool must be installed outside of the UKG Cloud, on a server that is under Customer’s control, therefore, the parties agree that the Health Extensions SLA referenced in Exhibit 3 and the UKG Cloud as detailed in this Services Description shall not apply to the Encryption Gateway Tool.

## 5.2 Customer's Responsibilities

Customer agrees to:

- (a) install, maintain, and use the Encryption Gateway Tool as part of the Subscription Services in accordance with the Encryption Gateway Documentation. Customer acknowledges that its failure to immediately apply updates to the Encryption Gateway Tool when such updates become available may: (i) compromise the security of Customer Data, including, Personal Data and PHI; and (ii) result in incompatibility between the Healthcare Extensions and the Encryption Gateway Tool, which could cause failures in Encrypting and un-Encrypting data, and affect the scope of the Subscription Services provided by UKG and its ability to adhere with its compliance programs, including those verified by the independent auditor report (i.e., SOC reports).
- (b) install and maintain the Encryption Gateway private key per the Encryption Gateway Documentation, and not share the Encryption Gateway private key with any third party who does not have a need to know, including not sharing the Encryption Gateway private key with UKG. Customer acknowledges that should Customer lose the key, any encrypted data will remain encrypted.
- (c) enter and maintain PHI only in the fields defined in the Healthcare Extensions Documentation; and to only send PHI data (e.g., screen shots containing PHI) to UKG by means of secure support channels for such data.
- (d) use unique user ID and passwords for all users of Healthcare Extensions.
- (e) configure Healthcare Extensions user's account to meet Customer's HIPAA policy requirements for complexity, length duration and lockout.
- (f) determine user access/authorization to the application level of the Solution and assure that the level of access and the user assigned roles and permission are appropriate, which includes periodic application level logical access review.
- (g) review application logs to meet Customer's HIPAA compliance program.
- (h) immediately notify UKG in the event Customer discovers a security issue with the Solution.
- (i) provide UKG resources with application-level accounts as reasonably needed to support the Healthcare Extensions, and not unreasonably withhold such access.

**Exhibit 1**  
**Cloud Services for Healthcare Extensions**

| Cloud Offering   |  |
|--|--|
| <p><b>Sub-processor for Healthcare Extensions:</b></p> <p>Cyxtera Technologies, Inc.<br/>BAC Colonnade Office Towers<br/>2333 Ponce De Leon Blvd, Suite 900<br/>Coral Gables, FL 33134 USA</p> <p><b>NOTE: Healthcare Extensions are deployed in datacenters in the USA ONLY.</b></p>  | <p>No data processed;<br/>co-location services only</p>  |
| <p><b>Environments:</b></p> <p>One standard Production and one Non-Production (Development) environment.<br/>Excludes Encryption Gateway software running at a location outside of the UKG Cloud, on a server that is in customer's control.</p>   | <p>Included.<br/>Additional non-production environments are available for additional fees.</p>                               |
| <p><b>Environment restoration:</b></p> <p>Restore of Production environment to one Non-Production environment once per week.<br/>Customer is responsible for requesting data to be moved from the Production environment to the Non-Production environment and for the contents of the data moved from the Production environment to the Non-Production environment.<br/>Excludes Encryption Gateway software running at a location outside of the UKG Cloud, on a server that is in customer's control.</p>   | <p>Included.<br/>More frequent restores or additional environments will be subject to additional time and material fees.</p> |
| <p><b>Connectivity to Service:</b></p> <p>Customer's users connect to applications via secure TLS connection over the internet. Cooperative efforts with customer IT staff may be required to enable access. UKG will assist with validating site connectivity but assumes no responsibility for customer internet connection or ISP relationships. UKG related Internet traffic cannot be filtered by proxy or caching devices on the client network. Exclusions must be added for the fully qualified domain names and public IP addresses assigned to the environments in the UKG Cloud. Applicable ports must be opened from customer network as described in product documentation.</p> | <p>Included</p>  |
| <p><b>Operating System and Database Software Management:</b></p> <p>Subscription Service of critical security patches, service packs and hot-fixes; maintenance of servers.<br/>Excludes Encryption Gateway software running at a location outside of the UKG Cloud, on a server that is in customer's control.</p>  | <p>Included</p>  |
| <p><b>Server Maintenance:</b></p> <p>Repair and replacement of defective or failed hardware and the installation of hardware upgrades.<br/>Excludes Encryption Gateway software running at a location outside of the UKG Cloud, on a server that is in customer's control.</p>   | <p>Included</p>  |
| <p><b>Subscription Service Updates:</b></p> <p>Services to perform technical tasks required to apply Subscription Service service packs, legislative updates (if applicable), point releases and version upgrades.<br/>Excludes Encryption Gateway software running at a location outside of the UKG Cloud, on a server in customer's control.</p>   | <p>Included</p>  |

| <b>Cloud Offering</b>   |          |
|---|----------|
| <p><b>Backups:</b><br/>Customer data is backed up daily. Database backups are replicated via encrypted connections to a second UKG Cloud datacenter. Backups are retained for the prior 28 days on a rotating basis. All historical employee and configuration data is stored in the rotating backups.</p> <p>Excludes Encryption Gateway software running at a location outside of the UKG Cloud, on a server in customer's control.</p> | Included |

**EXTENSIONS for HEALTHCARE EXTENSIONS**

**Cloud Guidelines and Assumptions**

| <b>Assumption</b>  |
|--|
| Estimated availability of Production server hardware in UKG Cloud is approximately 30 days after the Order Form is processed.  |
| Customer agrees to receive automatic updates to the Subscription Services.   |
| Subscription Services will support English only.   |
| Customer agrees not to conduct security testing, which includes but is not limited to penetration testing and vulnerability scanning.  |
| Customer agrees not conduct any sort of automated or manual performance testing of the Service.  |
| Retention policies must be configured in the Subscription Services. Setting retention policies will ensure that unnecessary system data (e.g. temp files, deleted records, empty rows, etc.) is routinely purged from the system and will help in managing database growth. Additionally, application audit log will retained for 30 days. |
| Customer will be required to sign a go-live milestone document confirming customer has completed its testing and is ready to go live with the UKG Healthcare Extensions.   |

**EXTENSIONS for HEALTHCARE EXTENSIONS**

**Upgrade Services**

The Subscription Services include services for UKG to execute tasks to apply point releases and version upgrades to customer's Subscription Services. Subscription Services are limited to those tasks which apply these updates to the Subscription Services. Subscription Services related to upgrade of Encryption Gateway Environment and Encryption Gateway software running at a location outside of the UKG Cloud on a server in customer's control are not included.

The table below reflects the included/excluded upgrade tasks.

|  |              |
|--|--------------|
| <b>Planning Phase</b>  |              |
| Customer/ UKG Introduction Call – up to 30 minutes   | Included     |
| Technical readiness & architecture review – UKG Cloud Environment  | Included     |
| Technical readiness & architecture review – Encryption Gateway environment   | Not Included |
| <b>Assessment Phase</b>  |              |
| Assessment of Interface Upgrades to UKG Dimensions   | Included     |
| Assessment of new features or changes to configuration   | Not included |
| Assessment of customs, custom interfaces and custom reports and development activities related thereto   | Not included |
| <b>Solution Upgrade / Build Phase</b>  |              |
| One (1) restore of Production database to Non-Production environment for the purpose of upgrade testing. Additional restores, if requested, shall be subject to additional time and material fees. | Included     |
| Upgrade Non-Production and Production environments to new point release or version.  | Included     |
| Upgrade of interface integration(s) to UKG Dimensions per features in product documentation, if applicable.  | Included     |
| Upgrade of integrations beyond integration to UKG Dimensions per features in product documentation.  | Not Included |

|  |                        |
|--|------------------------|
| Upgrade of any customs, custom interfaces and custom reports and development activities related thereto.   | Not Included           |
| Configuration of new features or functionality or changes to existing configuration  | Available for Purchase |
| Upgrade of Encryption Gateway environment and Encryption Gateway software running at a location outside of the UKG Cloud, on a server in customer's control. | Not Included           |
| <b>Test &amp; Certify Phase</b>  |                        |
| User acceptance testing (UAT) of upgraded environments, interfaces, custom reports, new features, etc.   | Not Included           |
| Develop customer-specific test cases   | Not Included           |
| Sign-off on upgraded Non-Production and Production Environments  | Customer               |
| <b>Deploy &amp; Support Phase</b>  |                        |
| Deployment Readiness Call – up to 30 minutes   | Included               |

*Note that new feature configuration, project management services, other Professional and Educational Services and training are not included as part of Upgrade Subscription Services, but may be purchased independently, if desired.*

*If not specifically noted, the customer should assume responsibility of the task and/or deliverable.*

**EXHIBIT 2**  
**Security and Disaster Recovery**

|  |                 |
|--|-----------------|
| <p><b>Security:</b></p> <p>UKG maintains a hosting environment that undergoes examinations from an independent auditor in accordance with the American Institute of Certified Public Accounts (AICPA) Trust Services Principles Section 100a, Trust Services for Security, Availability, Processing Integrity, Confidentiality and Privacy (i.e. SOC 2). The UKG Private Cloud is evaluated for the principles of Security, Availability and Confidentiality by the independent auditor. The UKG Private Cloud is located in data centers that undergo SSAE 18 examinations. Management access to the UKG Private Cloud is limited to authorized UKG support staff and customer authorized integrations. The security architecture has been designed to control appropriate logical access to the UKG Private Cloud to meet the Trust Services Principles of Security, Availability and Confidentiality. The Subscription Services provide the customer with the ability to configure application security and logical access per the customer's business processes. Additionally, an independent auditor provides an opinion on the design and operating effectiveness of controls to meet the security requirements of the Health Insurance Portability and Accountability Act Security Rule, which is available upon written request.</p> <p>In the event the customer identifies a security issue, the customer will notify UKG. For security purposes, customers are restricted from accessing the desktop, file systems, databases and operating system of the environments.</p> <p>Customer agrees not to upload payment card information, as the service is not certified for PCI DSS.</p> | <p>Included</p> |
| <p><b>Disaster Recovery Services:</b></p> <p>Customer environment and all customer data in the UKG Cloud are replicated to a secondary UKG Cloud data center. Disaster Recovery Services provide a Recovery Point Objective (RPO) of 12 hours and a Recovery Time Objective (RTO) of 24 hours.</p> <p>Any issues arising out of the Disaster Recovery event due to customer configuration/customization and/or customer third party software outside of the UKG Cloud is the responsibility of the customer to resolve.</p> <p>Excludes Encryption Gateway Tool running at a location outside of the UKG Cloud, on a server in customer's control.</p>   | <p>Included</p> |

**EXHIBIT 3**  
**Healthcare Extensions**  
**SERVICE LEVEL AGREEMENT (SLA)**

**Service Level Agreement:** The Subscription Services, in a production environment, are provided with the service levels described in this Exhibit A. SLAs are only applicable to production environments. SLAs will be available upon Customer's signature of UKG' Go Live Acceptance Form for Customer's production environment.

**99.75% Subscription Services Availability**

**Actual Subscription Services Availability %** = (Monthly Minutes (MM) minus Total Minutes Not Available (TM)) multiplied by 100) and divided by Monthly Minutes (MM), but not including Excluded Events

**SLA Credit Calculation:** An Outage will be deemed to commence when the Subscription Services are unavailable to Customer in Customer's production environment hosted by UKG and end when UKG has restored availability of the Subscription Services. Failure to meet the 99.75% Subscription Services Availability SLA, other than for reasons due to an Excluded Event, will entitle Customer to a credit as follows:

If, due to an Outage, the Subscription Service does not maintain 99.75% Availability, Customer is entitled to a credit to Customer's monthly invoice for the affected month, such credit to be equivalent to 3% of Customer's monthly PEPM Fees for every 1% of Availability below 99.75%, but in no event to exceed 100% of Customer's monthly PEPM Fees.

**"Outage"** means the accumulated time, measured in minutes, during which Customer is unable to access the Subscription Services for reasons other than an Excluded Event.

**"Excluded Event"** means any event that results in an Outage and is caused by (a) the acts or omissions of Customer, its employees, customers, contractors or agents; (b) the failure or malfunction of equipment, applications or systems not owned or controlled by UKG, including without limitation Customer Data, failures or malfunctions resulting from circuits provided by Customer, any inconsistencies or changes in Customer's source environment, including either intentional or accidental connections or disconnections to the environment; (c) Force Majeure events; (d) expected downtime during the Maintenance Periods described below; (e) any suspension of the Services in accordance with the terms of the Agreement to which this Exhibit A is attached; (f) the unavailability of required Customer personnel, including as a result of failure to provide UKG with accurate, current contact information; or (g) using an Subscription Services in a manner inconsistent with the Documentation for such Subscription Services.

**"Maintenance Period"** means scheduled maintenance periods established by UKG to maintain and update the Subscription Services, when downtime may be necessary, as further described below. The Maintenance Period is used for purposes of the SLA Credit Calculation; UKG continuously maintains the production environment on a 24x7 basis to reduce disruptions.

**Customer Specific Maintenance Period**

1. Customer will choose one of the following days of the week for their Maintenance Period: Saturday, Sunday, Wednesday or Thursday.
2. UKG will use up to six (6) hours in any two (2) consecutive rolling months (specifically: January and February; March and April; May and June; July and August; September and October; November and December) to perform Customer Specific Maintenance, excluding any customer requested Subscription Services updates. Downtime in excess of these six (6) hours will be deemed to be an Outage.
3. Customer Specific Maintenance will occur between 12am-6am EST.
4. Excluding any customer requested Subscription Services updates, UKG will provide notice for planned downtime via an email notice to the primary Customer contact so planning can be facilitated by Customer.
5. Customer Specific Maintenance Windows also include additional maintenance windows mutually agreed upon by Customer and UKG.
6. In absence of instruction from Customer, UKG will by default perform Maintenance in the time zone where the Data Center is located.

**Non-Customer Specific Maintenance Period**

UKG anticipates non-Customer Specific Maintenance to be performed with no or little (less than three hours per month) Customer downtime. If for any reason non-Customer Specific Maintenance requires downtime, UKG will provide as much notice as reasonably possible of the expected window in which this will occur.

Downtime in excess of three (3) hours per month for Non-Customer Specific Maintenance will be deemed to be an Outage.

**"Monthly Minutes (MM)"** means the total time, measured in minutes, of a calendar month commencing at 12:00 am of the first day of such calendar month and ending at 11:59 pm of the last day of such calendar month.

**"Total Minutes Not Available (TM)"** means the total number of minutes during the calendar month that the Subscription Services are unavailable as the result of an Outage.

**Reporting and Claims Process:** SLA Credits will not be provided if: (a) Customer is in breach or default under the Agreement at the time the Outage occurred; or (b) the Outage results from an Excluded Event.

UKG will provide Customer with a Subscription Services Availability report on a monthly basis for each prior calendar month. Within sixty (60) days of receipt of such report, Customer must request the applicable SLA Credit by written notice to UKG. Customer waives any right to SLA Credits not requested within this time period. All performance calculations and applicable SLA Credits are based on UKG records and data unless Customer can provide UKG with clear and convincing evidence to the contrary.

The Service Level Agreement in this Exhibit, and the related SLA Credits, apply on a per production environment basis. For the avoidance of doubt, Outages in one production environment may not be added to Outages in any other production environment for purposes of calculating SLA Credits.

Customer acknowledges that UKG manages its network traffic in part on the basis of Customer's utilization of the Subscription Services and that changes in such utilization may impact UKG's ability to manage network traffic. Therefore, notwithstanding anything else to the contrary, if Customer significantly changes its utilization of the Subscription Services than what is contracted with UKG and such change creates a material and adverse impact on the traffic balance of the UKG network, as reasonably determined by UKG, the parties agree to co-operate, in good faith, to resolve the issue.