SAP U.S. Benefits Administration by Benefitfocus
Supplemental Terms and Conditions

This Supplement is part of an Agreement for SAP Cloud Services between SAP and Customer and applies only to SAP U.S. Benefits Administration by Benefitfocus services to which Customer is subscribed ("Cloud Service"). Any documents referenced in this Supplement are available upon request.

1. CLOUD SERVICE

The Cloud Service enables customers to simplify the management of complex benefits processes, from shopping through enrollment and implementation to ongoing administration, to streamline benefits processes, and keeping up with regulatory requirements.

2. FEES

2.1. **Usage Metric**. The Usage Metric for the Cloud Service is Users. Users are individuals authorized to access the Cloud Service. For this Cloud Service, an individual with a unique active profile and whose data is processed by the Cloud Service is counted.

2.2. **Options**. Two options of the Cloud Service are available:

2.2.1. SAP U.S. Benefits Administration by Benefitfocus, full benefits option, is for employees that are eligible for at least one medical (excluding minimum essential coverage plans), dental, vision, or other IRC Section 125 benefit type configured within the Cloud Service. This option includes ten carrier interfaces, one payroll, one HR interface, and a client manager for support.

2.2.2. SAP U.S. Benefits Administration by Benefitfocus, voluntary benefits option, is for employees that are only eligible for enrolling in one or more non-IRC section 125 benefit types or one or more minimum essential benefit types configured within the Cloud Service. This option includes one payroll and one HR interface. Carrier interfaces will be included. This option also includes a minimum of 3 voluntary benefit types offered for the Cloud Service to be selected by Customer.

2.3. **SAP U.S. Benefits Administration by Benefitfocus, add-on for additional interfaces.** The Usage Metric for SAP U.S. Benefits Administration by Benefitfocus, add-on for additional interfaces is a connection per Additional Interface. Connection is a linkage between the Cloud Service and another system/technology. An Additional Interface means any data interface or connection to or from the Cloud Service (excluding those included in SAP U.S. Benefits Administration by Benefitfocus, full benefits option or SAP U.S. Benefits Administration by Benefitfocus, voluntary benefits option) utilizing the Cloud Service payMax, iMax, standard carrier API, or HIPAA 834 file standard specifications.

2.4. **SAP US Benefits Administration by Benefitfocus, reporting option for the Affordable Care Act (ACA).** The Usage Metric for SAP US Benefits Administration by Benefitfocus, reporting option for the Affordable Care Act (ACA) is Documents. A Document is a record of commercial transactional data managed via the Cloud Service. For this Cloud Service, the Document metric applies to any W-2 employees, retirees, or COBRA participants enrolled in self-insured coverage, or union covered employees that are configured within the solution during the applicable IRS reporting period. Fees are based on Documents that are configured within the Cloud Service. It is Customer's responsibility to provide any supplemental data needed in the required format as designated by SAP during implementation and thereafter, and review and approve any results prior to printing and filing forms with the IRS and applicable states. The Cloud Service includes a client manager for support.

3. ADDITIONAL TERMS.

3.1. The Data Privacy and Security – Data Controller to Data Processor Agreement referenced in or attached to the Order Form is superseded by the terms in **Attachment 1** to these Supplemental Terms and Conditions which is incorporated herein by reference.

3.2. The Cloud Service is only intended for processing data of United States-based employees. If Customer wishes to process data of non-United States based employees, Customer must contact SAP to enter into a separate

agreement relating to the processing of personal data of such employees. All data will be processed in data centers located in the United States.

3.3. Implementation services are required to configure the Cloud Service to meet Customer's business needs. These implementation services are not included in the Cloud Service.

3.4. Additional services included with the Cloud Service:

3.4.1. Year-round account management led by designated Client Success Manager (CSM) who will assist with ongoing software maintenance (including software releases), annual open enrollment management and support, legislative updates, and issue research/resolution as applicable.

3.4.2. Data exchange from client to and from HRIS/Payroll along with core medical and voluntary benefit providers. Additional fees could be incurred above the included standard carrier connections.

Attachment 1
To
Supplemental Terms and Conditions
For
SAP U.S. Benefit Administration by Benefitfocus
U.S. Data Protection Agreement

1. DEFINITIONS

"**SAP Affiliates**" shall mean any of SAP's affiliates and subsidiaries, meaning a corporation or other entity of which SAP owns, either directly or indirectly, more than fifty percent (50%) of the stock or other equity interests.

"**Data**" and/or "**data**" shall mean any information relating to an identified or identifiable natural or legal person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

"**Service**" shall mean any work or service which SAP provides to Customer or its Affiliates which incorporates the terms of this U.S. Data Protection Agreement by reference.

2. PURPOSE OF DATA TRANSFER; OWNERSHIP OF DATA

2.1. SAP will process Data from Customer to provide the Service to Customer and to create aggregate statistics about the use of the Service, which may be used by SAP and its partners to improve the Service.

2.2. As between Customer and SAP, all Data and data carriers provided to SAP from Customer and any copies, reproductions, summaries, analyses or extracts thereof or based thereon, including (without limitation) those made by SAP in performance of its obligations under the Agreement, are the property of Customer and shall be promptly returned to Customer upon any of the following events, whichever is earliest: (i) upon Customer's request; or (ii) upon completion of all tasks for which the respective Data was transferred to SAP; or (iii) upon expiry or termination of the Agreement. Alternatively, where Data and/or data carriers cannot be returned, or if Customer elects so, SAP shall destroy and certify to Customer in writing that he has destroyed all such Data and data carriers which otherwise would have to be returned in accordance with this Section 2.2.

2.3. This Service is only available within the United States and this Data Protection Agreement applies only to transfers of Data within the United States. Prior to any contractual data processing subject to EU Data Protection Directive 95/46/EC, including transfer of personal data outside of the European Union/European Economic Area, the parties agree to execute additional written agreements containing adequate regulations to protect the individuals' privacy and comply with applicable data protection laws.

2.4. To the extent that Customer transfers or provides any Data to SAP, Customer represents and warrants that Customer has collected such Data in accordance with applicable law.

3. ADDITIONAL OBLIGATIONS

3.1. For processing Data, SAP and its subprocessors shall only use personnel who are subject to a binding obligation to observe data secrecy or secrecy of telecommunications, to the extent applicable, pursuant to the applicable data protection law.

3.2. SAP shall ensure that any subcontractors, service providers or other entities processing Data subject to this Data Protection Agreement on behalf of SAP (hereinafter, "subprocessors") are required to have substantially similar protections for Data under this Agreement. SAP remains liable for the compliance of its subprocessors with applicable law. SAP shall reasonably cooperate with Customer in dealing with inquiries and requests relating to SAP's processing of Data within the context of a Service.

3.3. If Customer is a Covered Entity that will provide to SAP, in connection with consuming the Services, Protected Health Information that is subject to protection under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health

("HITECH)" Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 ("ARRA"), Pub. L. No. 111-5 (Feb. 17, 2009) and related regulations, the HIPAA Privacy Rule ("Privacy Rule"), Customer shall notify SAP and the parties agree to execute a Business Associate Agreement.

4. REPORTING OF VIOLATIONS; COMPLIANCE AUDITS

4.1. SAP will promptly report to Customer as soon as commercially feasible (a) any violations or reasonable suspicion that a violation of this Data Protection Agreement has occurred and (b) any actual or a reasonable suspicion of unauthorized access to Data.

4.2. For the production systems which run the Service itself and during the term of the Agreement SAP shall maintain, at its own expense, applicable certifications or audit reports. Unless provided otherwise in a Supplement, SAP engages an internationally recognized independent third party auditor to review the measures in place in protection of the Service(s). Certifications may be based on ISO 27001 or other standards (scope as defined in certificate). For certain SAP Cloud Services, SAP performs regular audits (at least annually) via certified auditors to provide a valid SOC 1 Type 2 (SSAE 16 or ISAE 3402) and/or SOC 2 Type 2 report. Audit reports are available through the third party auditor or SAP, as applicable. Upon Customer's request, SAP shall inform the Customer about the applicable certifications and audit standards available for the Service concerned.

4.3. If SAP fails to perform its audit obligations under Section 4.2 and has not provided sufficient evidence of its compliance after Customer's written request, Customer (or an independent third party auditor on its behalf that is subject to confidentiality obligations consistent with those in the Agreement) may audit SAP's control environment and security practices relevant to Data processed hereunder for Customer once in any twelve (12)-month period, with reasonable prior written notice (at least 60 days unless a data protection authority requires Customer's earlier control under applicable law) and under reasonable time, place and manner conditions.

4.4. Furthermore, (i) following an event set out in Section 4.1 above, or (ii) if Customer has reasonable ground to suspect the non-compliance of SAP with its obligations under this Exhibit, or (iii) if a further audit is required by Customer's data protection authority, Customer (or an independent third party auditor on its behalf that is subject to confidentiality obligations consistent with those in the Agreement) may audit SAP's control environment and security practices relevant to Data processed hereunder for Customer in accordance with applicable law.

4.5. SAP shall reasonably support Customer throughout these verification processes and provide Customer with the required information. Customer shall bear any costs (including SAP's internal resource based on then-current daily professional service rates per SAP's price list) for any efforts on SAP's side exceeding more than 4 hours per year.