RULES OF ENGAGEMENT
END USER DATA PROCESSING AGREEMENT ADDENDUM

End User Contact Name	
End User Contact Phone/Email	
InterSystems Advisor	
InterSystems Advisor Phone/Email	
Product/Version	
Service Period Start/End (dates)	
Service Description (“Service”) (include short description of Personal Data and WRC/TRC Problem Number)	
Transfer to U.S. or AU	◯ Permitted ◯ Not Permitted* *End User agrees and acknowledges that if data transfer is not permitted that End User waives rights to Service and InterSystems may deny Services without penalty should data transfer be necessary.
InterSystems Service Workforce Members (provide names)	

In addition to the obligations for End User and InterSystems in the End User Data Processing Agreement Addendum between the Parties related to the relevant EULSA, these Rules of Engagement (“RoE”) ensure that the Parties recognize when Data Protection Legislation compliance is associated with the Service for which InterSystems is a Data Processor to the extent that these RoE specifically indicate that InterSystems will have access to, use of, and actual processing of Personal Data to provide the Service.

End User Obligations

1. End User shall provide InterSystems Workforce Members, identified above, the following:
   a. Written copies of End User policy and procedure for Data Protection Legislation compliance requirements for End User; and
   b. Written notice of any limitations in End User’s notices and/or consent, any changes in, or revocation of, permission to use/disclose Personal Data or any restriction to the use/disclosure of Personal Data to which End User (or as appropriate, the relevant Controller) has agreed with the Data Subject(s) that may affect the Service to be provided.
2. End User shall:
   a. Represent and warrant that access to and use of Personal Data is required for InterSystems to provide the Service and shall not provide InterSystems direct and independent access to Personal Data;
   b. Limit any InterSystems access to and use of Personal Data to the minimum data necessary for InterSystems to provide the Service and, to the extent practicable, omit directly identifying Personal Data; and
   c. Use appropriate safeguards for transmitting Personal Data to InterSystems for the Service, including prohibiting the use of unencrypted email messages or file transfers.

InterSystems Obligations

1. InterSystems shall have InterSystems Workforce Members, identified above:
   a. Acknowledge End User policy and procedure for Data Protection Legislation compliance as part of working on the Service;
   b. Not request, access, or copy Personal Data unless required for the delivery of the Service to the End User;
   c. Not request individual or independent accounts on End User systems;
   d. Not transmit or disclosure Personal Data to anyone except for specifically identified End User personnel and InterSystems Workforce Members associated with this Service; and
   e. Use only encrypted or secure means with the default being use of WRC Direct or iService to transmit or disclose Personal Data.
2. InterSystems shall:
   a. Document any Service that requires use or disclosure of Personal Data and identify any WRC Direct or iService “ticket” associated with the Service as Elevated Security to provide necessary protections;
   b. At the conclusion of the Service, destroy or delete any Personal Data in its possession; and
   c. With regard to any data transfer to the U.S. or Australia, maintain a current executed version of the Standard Contractual Clauses for Controller to Controller transfers (EC document number C(2004) 5271).