DPA - RCM

ملحق (هـ) معالجة البيانات (DPA)

يُعد هذا الملحق جزءًا لا يتجزأ من الاتفاقية الرئيسية المبرمة بين الطرفين، ويُشار إليه باسم "ملحق معالجة البيانات الشخصية ."(DPA) ويُطبق هذا الملحق على معالجة البيانات الشخصية التي يقوم بها الطرف الأول نيابةً عن الطرف الثاني وفقًا لأحكام الاتفاقية الرئيسية.

لغايات هذا الملحق:

- **الطرف الأول :**شركة وصيل لنقل المعلومات الإلكترونية المحدودة، كما هو معرَّف في الاتفاقية الرئيسية، ويُشار إليه في هذا الملحق بـ **"الطرف الأول "**أو **"معالج البيانات."**
- **الطرف الثاني :**المنشأة الصحية/العميل، كما هو معرَّف في الاتفاقية الرئيسية، ويُشار إليه في هذا الملحق بـ**"الطرف الثاني "**أو **"جهة التحكم بالبيانات."**

ويُشار إلى الطرف الأول والطرف الثاني معاً بـ**"الطرفين."**

ويُعد اعتماد الطرف الثاني للاتفاقية الرئيسية قبولاً صريحاً وملزماً لجميع أحكام هذا الملحق، بما في ذلك أي نسخة منشورة أو محدثة على موقع الطرف الأول الإلكتروني.

ولغايات هذا الملحق:

- يُعد الطرف الثاني "جهة التحكم بالبيانات.(Controller) "
- ويُعد الطرف الأول "معالجًا للبيانات(Processor) "، فيما يتعلق بالبيانات الشخصية التي تتم معالجتها بموجب الاتفاقية الرئيسية.

ولغايات هذا الملحق، يُعد الطرف الثاني "جهة التحكم بالبيانات" (Controller)، ويُعد الطرف الأول "معالجًا للبيانات" (Processor)، وذلك فيما يتعلق بالبيانات الشخصية التي تتم **معالجتها بموجب اتفاقية تقديم الخدمات والمنتجات المبرمة بين الطرفين ("الاتفاقية الرئيسية").**

تمهيد

1. أبرم الطرفان اتفاقية تقديم خدمات ومنتجات إدارة دورة الإيرادات (RCM) والخدمات المرتبطة بها (**الاتفاقية الرئيسية**)والتي تنظّم العلاقة التعاقدية بينهما فيما يتعلق بتقديم الخدمات التقنية والتشغيلية والمالية الموضّحة في الاتفاقية وملاحقها.
2. يقتضي تنفيذ بعض خدمات الطرف الأول بموجب الاتفاقية الرئيسية قيامه بمعالجة بيانات شخصية تعود لمرضى أو مستفيدين أو موظفين أو ممثلين عن الطرف الثاني أو جهات أخرى، وذلك بالنيابة عن الطرف الثاني وبالنيابة عنه وبصفته جهة التحكم بالبيانات.

3. يهدف هذا الملحق") **ملحق معالجة البيانات الشخصية** "أو" **الملحق (هـ)** (إلى تنظيم التزامات الطرفين تجاه معالجة البيانات الشخصية بما يتوافق مع نظام حماية البيانات الشخصية في المملكة العربية السعودية ("PDPL") ولوائحه التنفيذية ولوائح نقل البيانات الشخصية خارج المملكة (اللوائح).
4. يُعد هذا الملحق جزءاً لا يتجزأ من الاتفاقية الرئيسية، ويُقرأ معها كوحدة واحدة، دون أن يترتب عليه أي انتقاص من الحقوق أو الصلاحيات المقررة للطرف الأول بموجب الاتفاقية الرئيسية، إلا بالقدر اللازم فقط للامتثال لأحكام نظام حماية البيانات الشخصية واللوائح الملزمة.

وبناءً على ما تقدم، اتفق الطرفان –وهما بكامل الأهلية الشرعية والنظامية– على ما يلي:

المادة (1): التعريفات والتفسير

1. **الاتفاقية الرئيسية:**
يقصد بها اتفاقية تقديم خدمات ومنتجات إدارة دورة الإيرادات (RCM) المبرمة بين الطرفين، بما في ذلك جميع ملاحقها الملحق رقم (أ)، الملحق رقم (ب)، الملحق رقم (ج)، الملحق رقم (د)، والملحق (هـ) الحالي وأي تعديلات مكتوبة لاحقة عليها.
2. **القانون المطبق واللو ائح:**
نظام حماية البيانات الشخصية السعودي (PDPL) ولوائحه التنفيذية، ولوائح وضوابط نقل البيانات الشخصية خارج المملكة، وأي تعليمات أو إرشادات تنظيمية صادرة عن الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) أو مكتب إدارة البيانات الوطنية (NDMO)أو أي جهة مختصة أخرى ذات علاقة.
3. **السلطة المختصة:**
الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) ومكتب إدارة البيانات الوطنية (NDMO) أو أي جهة تنظيمية أخرى تُمنَح صلاحية الإشراف على حماية البيانات الشخصية في المملكة.
4. **البيانات الشخصية، البيانات الحساسة، المعالجة، خرق البيانات الشخصية، الشخص المعني بالبيانات (موضوع البيانات)، المتحكم، المعالج:**
تكون لهذه المصطلحات المعاني المحددة لها في نظام حماية البيانات الشخصية ولوائحه التنفيذية.
5. **الأشخاص المصرح لهم:**
الأشخاص أو الفئات التي يحددها الطرف الثاني (جهة التحكم) في الملحق رقم (1) على أنهم مخوّلون بإصدار تعليمات مكتوبة للطرف الأول بخصوص معالجة البيانات الشخصية.
6. **الأغراض التجارية:**
تعني الأغراض المرتبطة بتقديم خدمات إدارة دورة الإيرادات (RCM) والخدمات التقنية والتشغيلية والتحليلية المنصوص عليها في الاتفاقية الرئيسية، وأي أغراض أخرى مشروعة يتم تحديدها في الملحق رقم.(1)
7. **الملاحق:**
تُعد الملاحق المرتبطة بهذا الملحق جزءاً لا يتجزأ منه، وتشمل على سبيل المثال لا الحصر:

- **الملحق رقم :(1)** أغراض ومعايير معالجة البيانات الشخصية والتفاصيل ذات الصلة.
- **الملحق رقم :(2)** البنود التعاقدية القياسية لنقل البيانات الشخصية (إن وُجدت).
- **الملحق رقم :(3)** تدابير الأمن الفني والتنظيمي.

8. في حال تعارض أو غموض في التفسير، يُعمل بما يلي:
   1. يُفسَّر هذا الملحق والاتفاقية الرئيسية بصورة تكاملية قدر الإمكان.
   2. في كل ما يتعلق بحماية البيانات الشخصية والامتثال الإلزامي لنظام حماية البيانات الشخصية واللوائح، يُقدَّم هذا الملحق بالقدر الضروري فقط لتحقيق الامتثال للنظام.
   3. فيما عدا ذلك، وفي حال وجود تعارض حقيقي بين نص هذا الملحق ونصوص الاتفاقية الرئيسية، **تكون الغلبة لأحكام الاتفاقية الرئيسية**، ولا يُفسّر أي نص في هذا الملحق بما ينتقص من الحقوق أو حدود المسؤولية أو الملكية أو الصلاحيات المقررة للطرف الأول في الاتفاقية الرئيسية.
   4. في حال وجود تعارض بين نص هذا الملحق وأي بنود تعاقدية قياسية منصوص عليها في الملحق رقم (2) فيما يخص نقل البيانات الشخصية خارج المملكة، تكون الغلبة للبنود القياسية بالقدر المطلوب فقط لنقل البيانات وفق النظام.

المادة (2): الأطراف وأدوارهم في حماية البيانات

1. يقر الطرفان بأن:
   - الطرف الثاني هو **"جهة التحكم بالبيانات (Data Controller)** "فيما يتعلق بالبيانات الشخصية التي يتم معالجتها على أساس الاتفاقية الرئيسية.
   - الطرف الأول هو **"معالج البيانات (Data Processor)** "فيما يتعلق بهذه البيانات، وذلك في حدود تنفيذ خدمات إدارة دورة الإيرادات والخدمات المساندة لها بموجب الاتفاقية الرئيسية وهذا الملحق.
2. يحتفظ الطرف الثاني بالمسؤولية عن:
   - تحديد أغراض ووسائل معالجة البيانات الشخصية.
   - الالتزام بتوفير أي إشعارات نظامية للمستفيدين والحصول على الموافقات النظامية اللازمة منهم –عند الاقتضاء– وفقاً لنظام حماية البيانات الشخصية.
   - صحة وسلامة التعليمات الخطية التي يوجّهها للطرف الأول، وعدم تعارضها مع النظام أو اللوائح.
3. يقر الطرف الثاني بأن جودة الخدمات المقدَّمة من الطرف الأول تعتمد على مدى التزام الطرف الثاني بتقديم بيانات صحيحة وكاملة وفي الوقت المناسب، وفقاً لما ورد في الاتفاقية الرئيسية، ولا سيما المادة (4) والمادة (15) منها.
4. **دون إخلال بما ورد أعلاه، ودون الإضرار بحقوق الطرف الأول المنصوص عليها في الاتفاقية الرئيسية، وبالأخص المادة:(8/4)** يحتفظ الطرف الأول بحقه في **استخدام البيانات ومعالجتها وتحويلها إلى بيانات مجمّعة أو مجهولة الهوية** لا يمكن من خلالها التعرف على أي شخص طبيعي، وله حق التصرف فيها (بما في ذلك بيعها أو ترخيصها أو مشاركتها) متى كانت هذه المعالجة متوافقة مع نظام حماية البيانات الشخصية ولا تؤدي إلى كشف أي بيانات شخصية، وذلك وفقاً لما ورد تفصيلاً في الاتفاقية الرئيسية.

المادة (3): التزامات الطرف الأول (معالج البيانات) في معالجة البيانات الشخصية

مع مراعاة ما ورد في الاتفاقية الرئيسية، يلتزم الطرف الأول بالآتي:

1. معالجة البيانات الشخصية **فقط في حدود الأغراض التجارية** ولتنفيذ الخدمات المنصوص عليها في الاتفاقية الرئيسية، وبناءً على تعليمات مكتوبة من الطرف الثاني، وذلك في إطار ما يسمح به النظام.
2. الالتزام بعدم استخدام البيانات الشخصية لأي غرض مستقل عن تنفيذ الخدمات، باستثناء ما يتصل بتحويلها إلى بيانات مجمّعة أو مجهولة الهوية والتصرف فيها وفقاً للمادة (4/2) أعلاه والمادة (4/8) من الاتفاقية الرئيسية.

3. إبلاغ الطرف الثاني دون تأخير غير مبرر إذا رأى أن تعليمات الطرف الثاني بشأن المعالجة قد تخالف نظام حماية البيانات الشخصية أو لوائحه.
4. الالتزام –قدر الإمكان ووفق ما هو متاح من معلومات– بمساعدة الطرف الثاني في الوفاء بالتزاماته النظامية تجاه:
   - حقوق أصحاب البيانات (الوصول، التصحيح، الحذف، تقييد المعالجة، الاعتراض، نقل البيانات...إلخ).
   - إعداد تقييمات تأثير حماية البيانات عند الاقتضاء.
   - التواصل مع الجهات التنظيمية المختصة، وذلك في الحدود الواقعية والمعقولة ودون تحميل الطرف الأول أي التزامات إضافية تتجاوز ما تقضي به الاتفاقية الرئيسية أو هذا الملحق.
5. الالتزام بالمحافظة على سرية البيانات الشخصية وعدم إفشائها إلا:
   - للعاملين أو المتعاقدين أو المعالِجين الفرعيين الذين تقتضي طبيعة عملهم الاطلاع عليها، مع إلزامهم بالتزامات سرية مناسبة، أو
   - إذا كان الإفشاء مطلوباً بموجب نظام واجب النفاذ أو بأمر من جهة قضائية أو جهة تنظيمية مختصة، مع إخطار الطرف الثاني متى كان ذلك مسموحاً به نظاماً.

المادة (4): موظفو الطرف الأول

يلتزم الطرف الأول بما يلي:

1. أن يكون أي موظف أو متعاون يطلع على البيانات الشخصية ملتزماً بالتزامات السرية المهنية، سواء بموجب عقد عمل أو اتفاق سرية أو سياسات داخلية ملزمة.
2. التحاق العاملين المعنيين بمعالجة البيانات الشخصية بالتدريب اللازم – وفقاً لسياسات الطرف الأول – على متطلبات حماية البيانات الشخصية، بالقدر المناسب لطبيعة عملهم.
3. توجيه العاملين والمعنيين بواجباتهم تجاه حماية البيانات وفق نظام حماية البيانات الشخصية وهذا الملحق والاتفاقية الرئيسية.

المادة (5): الأمن وحماية البيانات

1. يلتزم الطرف الأول بتطبيق **تدابير تقنية وتنظيمية مناسبة** لحماية البيانات الشخصية من:
   - الوصول أو الاستخدام أو التعديل أو الإفشاء غير المصرح به،
   - أو الفقد أو التلف أو التدمير العرضي أو غير المشروع.

   وذلك وفق ما هو موضح في **الملحق رقم (3): تدابير الأمن الفني والتنظيمي**.

2. يراعى في هذه التدابير مستوى المخاطر المرتبطة بطبيعة البيانات الشخصية وحساسيتها، وقد تشمل –على سبيل المثال لا الحصر:–
   - تطبيق التشفير الإلزامي للبيانات الشخصية أثناء النقل وعند التخزين، متى كانت البيانات ذات طبيعة حساسة – ومنها البيانات الصحية – وبما يتوافق مع متطلبات نظام حماية البيانات الشخصية ولوائحه التنفيذية؛
   - آليات ضبط الصلاحيات والوصول؛
   - النسخ الاحتياطي واستعادة البيانات؛
   - مراقبة الدخول إلى الأنظمة؛
   - اختبار وتقييم كفاءة الضوابط بشكل دوري.

3. لا يُفسَّر أي التزام وارد في هذه المادة على أنه تعهد بتحمل مسؤولية مطلقة عن أي حادث أمني، بل تُقيَّم المسؤولية وفقاً لحدود المسؤولية المتفق عليها في الاتفاقية الرئيسية وبالأخص المادة.(15/6)

المادة (6): خرق البيانات الشخصية

1. يلتزم الطرف الأول بإخطار الطرف الثاني **فورعلم الطرف الأول بالو اقعة** بأي من الحالات الآتية المتعلقة بالبيانات الشخصية الخاضعة لهذا الملحق:
   - فقدان أو إتلاف أو تلف أو فساد جوهري للبيانات الشخصية؛
   - معالجة غير مصرّح بها أو غير قانونية؛
   - أو حادث خرق بيانات شخصية بالمفهوم الوارد في نظام حماية البيانات الشخصية.
2. يتضمّن الإخطار –قدر الإمكان– المعلومات التالية:
   - وصفاً لطبيعة الحادث وفئات البيانات المتأثرة وعدد السجلات التقريبي؛
   - الآثار أو النتائج المحتملة؛
   - الإجراءات التصحيحية أو الوقائية المتخذة أو المقترحة.
3. يتعاون الطرف الأول مع الطرف الثاني –في حدود المعقول– للتحقيق في الحادث وتخفيف آثاره، وذلك دون أن يترتب على الطرف الأول أي التزامات إضافية تتجاوز حدود المسؤولية المنصوص عليها في الاتفاقية الرئيسية وهذا الملحق.
4. يظل للطرف الثاني الحق في تحديد ما إذا كان يلزم إخطار أصحاب البيانات أو الجهات التنظيمية المختصة، وفقاً للنظام، مع مراعاة أن تنفيذ ذلك يقع ضمن مسؤوليات جهة التحكم (الطرف الثاني).

المادة (7): نقل البيانات الشخصية

1. يلتزم الطرف الأول بعدم نقل البيانات الشخصية خارج المملكة العربية السعودية إلا وفق الضوابط المنصوص عليها في نظام حماية البيانات الشخصية ولوائحه ولوائح نقل البيانات، وبالقدر اللازم لتقديم الخدمات أو تشغيل الأنظمة أو النسخ الاحتياطي أو غير ذلك من الأغراض المشروعة المرتبطة بالاتفاقية الرئيسية. ولا يقوم الطرف الأول بأي نقل فعلي للبيانات الشخصية خارج المملكة إلا بناءً على موافقة موثقة من الطرف الثاني، سواء كانت هذه الموافقة ضمن هذا الملحق أو من خلال تعليمات مكتوبة أو مراسلات رسمية بين الطرفين، وذلك دون إخلال بالالتزامات المنصوص عليها في نظام حماية البيانات الشخصية ولوائحه ذات العلاقة.
2. يقر الطرف الثاني ويمنح بموجب هذا الملحق موافقة مسبقة عامة على استخدام الطرف الأول لمزودي خدمات ومعالِجين فرعيين – داخل المملكة أو خارجها – متى كان ذلك ضرورياً أو مناسباً لتقديم الخدمات محل الاتفاقية، شريطة أن يلتزم هؤلاء المعالِجون الفرعيون بتدابير حماية بيانات لا تقل عن الحد المنصوص عليه في هذا الملحق والأنظمة ذات الصلة، وأن يلتزموا تعاقدياً بذات الالتزامات الجوهرية المفروضة على الطرف الأول بموجب هذا الملحق في حدود ما يتعلق بمعالجة البيانات الشخصية. ويلتزم الطرف الأول بإشعار الطرف الثاني عند إضافة فئة جديدة من فئات المعالِجين الفرعيين، متى كان ذلك عملياً.
3. في حال تم نقل البيانات الشخصية أو استضافتها خارج المملكة، يلتزم الطرف الأول بالتأكد من توفر مستوى حماية نظامي كافٍ للبيانات وفق متطلبات نظام حماية البيانات الشخصية ولوائح نقل البيانات، بما في ذلك الالتزام بالضوابط والتعليمات الصادرة عن الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) والجهات المختصة، والتأكد من أن أي جهة خارجية تتم معها المعالجة أو الاستضافة ملتزمة – تعاقدياً – بذات الالتزامات الجوهرية المنصوص عليها في هذا الملحق وفي الاتفاقية الرئيسية، وذلك في حدود ما يتعلق بحماية البيانات الشخصية.

4. يحق للطرف الأول –دون الحاجة إلى موافقة منفردة في كل مرة:–
   - إبرام عقود مكتوبة مع معالِجين فرعيين تتضمن التزامات حماية البيانات؛
   - استخدام آليات النقل النظامية المعتمدة (مثل البنود التعاقدية القياسية أو قرارات الملاءمة) عند الاقتضاء.
5. متى كان ذلك عملياً، يجوز للطرف الأول تزويد الطرف الثاني بقائمة عامة بالفئات الرئيسية للمعالِجين الفرعيين أو أماكن استضافة الأنظمة، بناءً على طلب مكتوب من الطرف الثاني، دون الإخلال بسرية ترتيبات الطرف الأول مع مزودي الخدمات أو أسرار أعماله.
6. يبقى الطرف الأول مسؤولاً عن اختيار المعالِجين الفرعيين بحسن نية وبما يتوافق مع النظام، **مع بقاء حدود مسؤوليته خاضعة للمادة (6/15) من الاتفاقية الرئيسية**.

المادة (8): الشكاوى وحقوق أصحاب البيانات

1. يلتزم الطرف الأول –في حدود ما يتاح له من معلومات وإمكانات– بمساندة الطرف الثاني عند تلقيه طلبات من أصحاب البيانات (مثل طلب الوصول، التصحيح، الحذف، تقييد المعالجة، نقل البيانات)، وذلك بالقدر اللازم والمتناسب لطبيعة الخدمات.
2. في حال تلقى الطرف الأول مباشرة أي طلب من صاحب بيانات يتعلق بحق من حقوقه النظامية، يحيل الطرف الأول الطلب –متى أمكن– إلى الطرف الثاني، بوصفه جهة التحكم المختصة بالرد النظامي.
3. لا يلتزم الطرف الأول بالتواصل المباشر مع أصحاب البيانات للرد على هذه الطلبات، إلا إذا تم الاتفاق على ذلك كتابياً أو تطلبه النظام صراحة.

المادة (9): مدة الملحق وعلاقته بالاتفاقية الرئيسية

1. يسري هذا الملحق طوال مدة سريان الاتفاقية الرئيسية وأي مدد تجديد لها، ويظل نافذاً ما دام الطرف الأول يحتفظ بأي بيانات شخصية خاضعة له بموجب الاتفاقية الرئيسية، في الحدود المسموح بها نظاماً.
2. لا يُعد انتهاء أو إنهاء الاتفاقية الرئيسية سبباً لإعفاء أي طرف من التزاماته المتعلقة بسرية المعلومات وحماية البيانات الشخصية، والتي تستمر طالما بقيت البيانات تحت حيازة أو سيطرة أي من الطرفين، وذلك وفقاً للمادة (7/8) من الاتفاقية الرئيسية.

المادة (10): إعادة البيانات الشخصية أو حذفها بعد انتهاء العلاقة

مع مراعاة أحكام الاتفاقية الرئيسية، لا سيما ما يتعلق بتحصيل الذمم واستمرارية بعض الالتزامات بعد الإنهاء، يراعى ما يلي:

1. يجوز للطرف الثاني أن يطلب –خلال مدة معقولة بعد انتهاء الاتفاقية الرئيسية– تزويده بنسخة من البيانات الشخصية التي تمت معالجتها نيابة عنه، في حدود ما هو متاح ومعقول فنياً وتشغيلياً، وبالصيغة التي يحددها الطرف الأول.
2. مع مراعاة الفقرة التالية، يقوم الطرف الأول بحذف أو إتلاف البيانات الشخصية الخاضعة لهذا الملحق أو إخفاء هويتها بشكل لا يمكن معه إعادة التعرف على أصحابها، وذلك خلال مدة معقولة بعد انتهاء العلاقة التعاقدية، ووفقاً للتعليمات المكتوبة من الطرف الثاني متى تم تزويد الطرف الأول بها، وبما لا يتعارض مع التزامات الطرف الأول النظامية أو التعاقدية أو حقوقه النظامية في الدفاع عن نفسه أو إثبات حقوقه
3. يجوز للطرف الأول الاحتفاظ ببعض البيانات أو السجلات التي تحتوي على بيانات شخصية في الحالات التالية:
   - إذا كان الاحتفاظ مطلوباً بموجب نظام واجب النفاذ أو تعليمات جهة تنظيمية مختصة؛
   - إذا كان الاحتفاظ لازماً لإثبات حق أو دفاع عن مطالبة أو نزاع قائم أو متوقع؛

- أو إذا تم تحويل البيانات إلى بيانات مجمّعة أو مجهولة الهوية وفقاً للمادة (4/2) من هذا الملحق والمادة (4/8) من الاتفاقية الرئيسية.

4. لا يترتب على أي حذف أو إعادة للبيانات الشخصية إسقاط أو إنقاص أي من المستحقات المالية للطرف الأول أو التزاماته أو حقوقه الأخرى بموجب الاتفاقية الرئيسية.

المادة (11): التدقيق والتوثيق

1. يلتزم الطرف الأول بالاحتفاظ بسجلات مناسبة عن أنشطة معالجة البيانات الشخصية التي يجريها نيابة عن الطرف الثاني، بالقدر الذي يقتضيه نظام حماية البيانات الشخصية ولوائحه.
2. متى طلب الطرف الثاني –وخاصة في حال وجود متطلبات نظامية أو رقابية– معلومات عامة عن التدابير الأمنية المطبقة لدى الطرف الأول، فيجوز للطرف الأول تزويده **بوثائق أو تقارير ملخصة** (مثل شهادات الاعتماد أو ملخصات تقارير التدقيق الأمنية)، دون الإخلال بسريته التجارية أو كشف تفاصيل حساسة عن أنظمته أو بنيته التحتية.
3. يجوز للطرف الثاني –عند وجود متطلبات نظامية أو رقابية– طلب تزويده بمعلومات أو وثائق مناسبة تثبت امتثال الطرف الأول لمتطلبات حماية البيانات، بما في ذلك مراجعات عن بُعد أو مراجعات مستندية، وذلك دون المساس بأمن الطرف الأول أو أسرار أعماله. ولا يتم إجراء أي تدقيق ميداني لدى الطرف الأول إلا بموافقة خطية مسبقة من الطرف الأول، وتحديد النطاق والإجراءات كتابة، وبما لا يتعارض مع سياسات الطرف الأول الأمنية أو التزامات السرية للغير..

المادة (12): الملكية الفكرية والبيانات المجمّعة

1. لا ينشئ هذا الملحق أي نقل لملكية الأنظمة أو المنصات أو البرمجيات أو لوحات المؤشرات أو أدوات التحليل أو التقارير التي يوفرها الطرف الأول، وتظل هذه الحقوق **ملكية حصرية للطرف الأول** وفقاً للمادة (8/8) من الاتفاقية الرئيسية.
2. يقر الطرف الثاني صراحة بحق الطرف الأول في استخدام ومعالجة البيانات وتحويلها إلى بيانات إحصائية أو مجمّعة أو مجهولة الهوية، والتصرف فيها تجارياً أو فنياً، طالما لم تعد هذه البيانات قابلة لأن تُنسب إلى شخص طبيعي محدد أو قابل للتعرّف عليه بشكل مباشر أو غير مباشر، وطالما تمت المعالجة وفقاً لنظام حماية البيانات الشخصية واللوائح ذات الصلة.

المادة (13): حدود المسؤولية والتعويض

1. لا يترتب على هذا الملحق إنشاء أي التزامات تعويضية إضافية على الطرف الأول تتجاوز ما هو منصوص عليه في الاتفاقية الرئيسية.
2. تخضع أي مسؤولية مالية أو نظامية تنشأ عن هذا الملحق –بما في ذلك ما يتعلق بمعالجة البيانات الشخصية –**لحدود المسؤولية المتفق عليها في الاتفاقية الرئيسية، ولا سيما المادة(15/6)** ، ولا يجوز بأي حال تجاوز تلك الحدود إلا بالقدر الذي يفرضه النظام صراحة.
3. يبقى كل طرف مسؤولاً عن التزامه بالأنظمة ذات العلاقة في حدود دوره (جهة تحكم أو معالج)، وبالقدر الذي تتحقق فيه علاقة سببية بين فعله أو امتناعه والضرر المتمسك به، مع مراعاة أحكام الاتفاقية الرئيسية في هذا الشأن.

المادة (14): القانون الحاكم والاختصاص القضائي

1. تخضع أحكام هذا الملحق –فيما لم يرد فيه نص خاص– لأحكام الاتفاقية الرئيسية، وللأنظمة واللوائح المعمول بها في المملكة العربية السعودية ذات الصلة بحماية البيانات، وعلى رأسها نظام حماية البيانات الشخصية ولوائحه التنفيذية.
2. يكون الاختصاص في نظر أي نزاع ينشأ عن تفسير أو تطبيق هذا الملحق للمحكمة المختصة في مدينة الرياض، وذلك وفقاً لما ورد في المادة (12) من الاتفاقية الرئيسية.

المادة (15): أحكام ختامية

1. يُعد هذا الملحق (هـ) جزءاً لا يتجزأ من الاتفاقية الرئيسية، ويُعمل به من تاريخ توقيعه من الطرفين أو من تاريخ نفاذ الاتفاقية الرئيسية – أيهما أبعد – ما لم يُتفق على غير ذلك كتابةً.
2. في حال تعارض أي نص في هذا الملحق مع نصوص الاتفاقية الرئيسية، تكون الأفضلية لنص الاتفاقية الرئيسية، **إلا في الحدود التي يكون فيها نص هذا الملحق مطلوباً للامتثال الإلزامي لنظام حماية البيانات الشخصية واللو ائح المرتبطة به**.
3. لا يُعد أي تعديل على هذا الملحق صحيحاً وملزماً إلا إذا كان بموجب وثيقة مكتوبة وموقّعة من الطرفين.
4. حرر هذا الملحق من نسختين أصليتين متطابقتين، بيد كل طرف نسخة، ويجوز للطرف الأول إصدار نسخ إلكترونية أو رقمية منها يُعتد بها نظاماً أسوة بما ورد في المادة (21) من الاتفاقية الرئيسية.

الملحق رقم (1) – أغراض ومعايير معالجة البيانات الشخصية

هذا الملحق جزء من ملحق معالجة البيانات الشخصية الملحق (هـ) ، ويُستخدم لتحديد تفاصيل المعالجة التي يقوم بها الطرف الأول نيابةً عن الطرف الثاني.

1. موضوع المعالجة

- تقديم خدمات إدارة دورة الإيرادات (RCM) والخدمات التقنية والتشغيلية والتحليلية المرتبطة بها، بما في ذلك:
  - التدقيق الطبي والتقني للمطالبات.
  - تجهيز ورفع المطالبات لشركات التأمين وشركات إدارة المطالبات.(TPAs)
  - إدارة التحصيل والمطابقة المالية.
  - إدارة الأهلية والموافقات الطبية.
  - إدارة منافع الصيدلية.(PBM)
  - التقارير ولوحات المؤشرات والتحليلات.

2. مدة المعالجة

- طوال مدة سريان الاتفاقية الرئيسية وأي مدد تجديد لها،
- مع استمرار بعض المعالجات أو الاحتفاظ بالبيانات بالقدر المسموح به نظاماً وبعد انتهاء العلاقة، وفقاً للمادة (10) من هذا الملحق وأحكام الاتفاقية الرئيسية.

3. غرض المعالجة والأغراض التجارية

- تمكين الطرف الثاني من:
  - إدارة دورة الإيرادات بكفاءة (مطالبات، تحصيل، مطابقة مالية).
  - تحسين جودة الرفع الطبي والتقني وتقليل نسب الرفض.
  - إدارة عمليات الموافقات والأهلية إلكترونياً.
  - إدارة وصفات الأدوية ومنافع الصيدلية.
  - الحصول على تقارير مالية وتشغيلية وتحليلية تساعد في اتخاذ القرار.
- تشمل المعالجة –على سبيل المثال لا الحصر:–
  - جمع واستقبال البيانات من أنظمة الطرف الثاني أو منصات الربط.
  - تخزين وتنظيم البيانات في أنظمة الطرف الأول.
  - استخدام البيانات في المعالجة التشغيلية اليومية (التدقيق، المطالبات، التحصيل).
  - إنشاء تقارير ولوحات مؤشرات مبنية على البيانات.
  - تحويل البيانات إلى بيانات مجمّعة أو مجهولة الهوية لأغراض التحليل الإحصائي أو التجاري، بما لا يخالف المادة (4/2) من الملحق والاتفاقية الرئيسية.

4. فئات البيانات الشخصية

- بيانات مرضى ومستفيدين:
  - الاسم الرباعي/الثلاثي.
  - رقم الهوية/الإقامة/رقم الملف الطبي.
  - بيانات التواصل (الهاتف، البريد الإلكتروني – إن وجدت).
  - بيانات التأمين (شركة التأمين، رقم الوثيقة، فئة التغطية، رقم العضوية).
  - بيانات المطالبات (التشخيص، الخدمات الطبية المقدمة، الأكواد الطبية، تاريخ الخدمة، المبالغ، نسب التحمل).
  - بيانات الموافقات الطبية (الأهلية، نتائج التحقق، الموافقات/الرفض).
- بيانات موظفي أو منسوبي الطرف الثاني ذات الصلة بتنفيذ الخدمات (إن وجدت):
  - الاسم والوظيفة.
  - بيانات التواصل المهنية.
  - بيانات الحسابات الممنوحة للدخول على الأنظمة.
- بيانات مالية مرتبطة بالمطالبات:
  - مبالغ المطالبات والمدفوعات.
  - تواريخ التحويلات.
  - أرقام إشعارات الدفع والمطابقة.

5. فئات أصحاب البيانات (موضوعات البيانات)

- المرضى والمستفيدون من خدمات الطرف الثاني.
- المؤمن لهم لدى شركات التأمين المتعاقدة مع الطرف الثاني.
- موظفو ومنسوبو الطرف الثاني المرتبطون بتنفيذ الخدمات (أطباء، إداريون، موظفو مطالبات ومالية وتقنية).
- ممثلو شركات التأمين أو شركات إدارة المطالبات، بقدر ما يُسجَّل في أنظمة الطرف الأول (مثل بيانات التواصل المهنية).

6. الأشخاص المصرح لهم بإعطاء التعليمات

- أي شخص آخر يحدده الطرف الثاني خطياً أو عبر قنوات رسمية متفق عليها بين الطرفين.

7. معالجة البيانات خارج المملكة والآلية النظامية (إن وُجدت)

إن تم نقل أو استضافة بعض البيانات خارج المملكة في سياق تقديم الخدمات، فيتم ذلك وفق ما يلي:

- الالتزام بضوابط نظام حماية البيانات الشخصية ولوائح نقل البيانات الشخصية.
- استخدام إحدى الآليات النظامية المعتمدة، مثل:
  - استضافة في دولة تعترف بها الجهة المختصة كدولة ذات مستوى حماية ملائم؛ أو
  - تطبيق بنود تعاقدية قياسية (SCC) مع مزود الخدمة الخارجي؛ أو
  - أي آلية أخرى تعتمدها سدايا NDMO/مستقبلاً.

الملحق رقم (2) – نقل البيانات الشخصية خارج المملكة والبنود التعاقدية القياسية

1. مبدأ عام

- الأصل أن تتم معالجة البيانات الشخصية داخل المملكة قدر الإمكان.
- لا يتم نقل البيانات الشخصية أو إتاحتها خارج المملكة إلا في الحالات التي تسمح بها الأنظمة واللوائح ذات الصلة وبالقدر الضروري لتقديم الخدمات أو تشغيل الأنظمة أو النسخ الاحتياطي أو الدعم الفني.

2. أسس وضوابط النقل

- عند نقل البيانات الشخصية خارج المملكة، يلتزم الطرف الأول بالآتي:
  1. التأكد من أن النقل يتم إلى دولة أو جهة تتوافر فيها حماية كافية للبيانات، وفق ما تقرره الجهة المختصة، أو
  2. تطبيق أحد الأطر النظامية المسموح بها لنقل البيانات، مثل:
     - البنود التعاقدية القياسية المعتمدة من سدايا(SCCs) ، إن وُجدت.
     - القواعد المؤسسية الملزمة(Binding Corporate Rules) ، عند توفرها.
     - أي آلية نظامية أخرى تعتمدها الجهات المختصة.

3. البنود التعاقدية القياسية(SCCs)

- عند الحاجة لتطبيق بنود تعاقدية قياسية لنقل البيانات الشخصية، يجوز للطرف الأول –وبتفويض من الطرف الثاني– إبرام هذه البنود مع مزودي الخدمات الخارجيين المعنيين بنقل أو استضافة البيانات، بما يتوافق مع النماذج المعتمدة من الجهات المختصة.
- تُعتبر هذه البنود –متى تم إبرامها– جزءاً مكملاً لهذا الملحق، ويمكن حفظها أو الإشارة إليها في اتفاقيات منفصلة (مثل اتفاقية مستوى الخدمة/اتفاقية الاستضافة).

4. توثيق الجهات الخارجية (إن وُجدت)

يمكن للطرف الأول تزويد الطرف الثاني –عند الطلب وبالقدر المناسب– بمعلومات عامة عن فئات مزودي الخدمة الخارجيين أو مناطق الاستضافة ذات الصلة بنقل البيانات الشخصية، دون الإخلال بسرية التعاقدات أو أسرار أعمال الطرف الأول.

الملحق رقم (3) – تدابير الأمن الفني والتنظيمي

1. ضوابط الوصول المادي

- حماية مراكز البيانات والمكاتب التي تحتوي على أنظمة أو وسائط تخزين بيانات شخصية، من خلال:
  - أنظمة دخول بالبطاقات أو بصمة أو وسائل تحقق أخرى.
  - كاميرات مراقبة في المواقع الحساسة.
  - تقييد الدخول إلى الفرق المصرح لها فقط.

2. ضوابط الوصول إلى الأنظمة

- إدارة حسابات وصلاحيات المستخدمين وفق مبدأ أقل صلاحية.(Least Privilege)
- استخدام كلمات مرور قوية وأنظمة مصادقة متعددة العوامل عند الاقتضاء.
- إلغاء أو تعديل صلاحيات المستخدمين عند تغير مهامهم أو انتهاء علاقتهم بالطرف الأول.

3. ضوابط الوصول إلى البيانات

- تقييد الاطلاع على البيانات الشخصية للعاملين أو المتعاقدين الذين تقتضي مهامهم العملية ذلك فقط.
- تسجيل ومراقبة عمليات الدخول والاطلاع على السجلات الحساسة.
- تطبيق سياسات "الحاجة إلى المعرفة.(Need-to-Know) "

4. ضوابط نقل البيانات

- استخدام بروتوكولات اتصال آمنة) مثل (HTTPS/VPN عند تبادل البيانات مع الطرف الثاني أو الجهات المرتبطة.
- تشفير البيانات أثناء النقل كلما كان ذلك مناسباً فنياً وعملياً.
- توثيق واجهات الربط التقني (APIs/Integrations) وتأمينها.

5. ضوابط إدخال ومعالجة البيانات

- تتبع العمليات الجوهرية (مثل إنشاء أو تعديل أو حذف سجلات حساسة) من خلال سجلات تدقيق.(Audit Logs)
- التحقق من صحة البيانات المدخلة قدر الإمكان لتقليل الأخطاء.
- وجود ضوابط تفويض/مراجعة لعمليات ذات أثر كبير (مثل المعاملات المالية).

6. النسخ الاحتياطية واستمرارية العمل

- تنفيذ آليات نسخ احتياطي دوري للبيانات والأنظمة الحرجة.
- اختبار خطط استعادة البيانات واستمرارية الأعمال بشكل دوري كلما أمكن.
- تخزين النسخ الاحتياطية في مواقع آمنة.

7. عزل البيانات

- عزل بيانات العملاء عن بعضهم البعض منطقياً أو من خلال طبقات صلاحيات وفق تصميم النظام.
- عند استخدام بيئات اختبار أو تطوير، يتم – قدر الإمكان – استخدام بيانات منزوعة الهوية أو مموّهة، أو تطبيق تدابير تحمي البيانات من الوصول غير المصرح به.

8. إدارة الثغرات والتحديثات

- تحديث الأنظمة والتطبيقات بشكل دوري لسد الثغرات الأمنية المعروفة.
- إجراء فحوصات دورية للثغرات (Vulnerability Scans) متى كان ذلك مناسباً.
- وجود إجراءات استجابة للأحداث الأمنية (Incident Response) للتعامل مع الحوادث عند وقوعها.

Appendix (E): Data Processing Addendum (DPA)

This Addendum constitutes an integral and inseparable part of the Main Agreement executed between the Parties and shall be referred to as the "Data Processing Addendum (DPA)". This DPA governs the Processing of Personal Data performed by the First Party on behalf of the Second Party in accordance with the terms of the Main Agreement.

For the purposes of this Addendum:

- **First Party:** Waseel ASP for Electronic Information Transmission (LTD.), as defined in the Main Agreement, and referred to in this Addendum as the **"First Party"** or the **"Data Processor"**.
- **Second Party:** The healthcare facility/customer, as defined in the Main Agreement, and referred to in this Addendum as the **"Second Party"** or the **"Data Controller"**.

The First Party and the Second Party may hereinafter be referred to collectively as the **"Parties"**.

Execution of the Main Agreement by the Second Party constitutes an explicit and binding acceptance of all provisions of this DPA, including any version published or updated on the First Party's official website**.**

For the purposes of this Addendum:

- The Second Party is the **"Data Controller"**.
- The First Party is the **"Data Processor"** in relation to the personal data processed under the Master Agreement.

For the purposes of this Addendum, the Second Party shall be deemed the **Data Controller**, and the First Party shall be deemed the **Data Processor**, in relation to the personal data processed under the Agreement for the Provision of Services and Products entered into between the Parties (the **"Master Agreement"**).

Preamble

1. The Parties have entered into an Agreement for the Provision of Revenue Cycle Management (RCM) Services and related products and services (the **"Master Agreement"**), which governs their contractual relationship in relation to the technical, operational, and financial services described in the Master Agreement and its Appendices.
2. The performance of some of the First Party's services under the Master Agreement requires the First Party to process personal data relating to patients, beneficiaries, employees, representatives of the Second Party, or other parties, on behalf of and for the account of the Second Party in its capacity as Data Controller.
3. This Addendum (the **"Data Processing Addendum"** or **"Appendix (E)"**) aims to regulate the Parties' obligations regarding the processing of personal data in accordance with the Personal Data Protection Law applicable in the

Kingdom of Saudi Arabia (**PDPL**), its Implementing Regulations, and the Regulations on the Transfer of Personal Data outside the Kingdom (together, the **Regulations**).

4. This Addendum forms an integral part of the Master Agreement and shall be read together with it as a single instrument, without in any way diminishing or limiting any rights or powers granted to the First Party under the Master Agreement, except to the minimum extent required to comply with the Personal Data Protection Law and mandatory Regulations.

In light of the foregoing, and with both Parties having full legal and Sharia capacity, they agree as follows:

Article (1): Definitions and Interpretation

1. **Master Agreement**
   Means the Agreement for the Provision of Revenue Cycle Management (RCM) Services and Products entered into between the Parties, including all of its Appendices: Appendix (A), Appendix (B), Appendix (C), Appendix (D), this Appendix (E), and any subsequent written amendments thereto.
2. **Applicable Law and Regulations**
   The Saudi Personal Data Protection Law (PDPL), its Implementing Regulations, the Regulations governing the transfer of personal data outside the Kingdom, and any circulars, guidelines, or regulatory instructions issued by the Saudi Data & Artificial Intelligence Authority (SDAIA), the National Data Management Office (NDMO), or any other competent authority.
3. **Competent Authority**
   SDAIA, NDMO, and any other regulatory body granted authority over personal data protection in the Kingdom.
4. **Personal Data, Sensitive Data, Processing, Personal Data Breach, Data Subject, Controller, Processor**
   Shall have the meanings ascribed to them under the Personal Data Protection Law and its Implementing Regulations.
5. **Authorized Persons**
   The persons or categories of persons designated by the Second Party (as Controller) in **Annex (1)** as being authorized to issue written instructions to the First Party regarding the processing of personal data.
6. **Business Purposes**
   The purposes related to the provision of Revenue Cycle Management (RCM) services and the related technical, operational, and analytical services set out in the Master Agreement, and any other lawful purposes specified in **Annex (1)**.
7. **Annexes**
   The annexes attached to this Addendum form an integral part hereof, including, without limitation:

- **Annex (1):** Personal Data Processing Purposes and Parameters, and related details;
- **Annex (2):** Cross-Border Data Transfer and Standard Contractual Clauses (if any);
- **Annex (3):** Technical and Organizational Security Measures.

8. **In the event of any conflict or ambiguity in interpretation, the following shall apply:**
    1. This Addendum and the Master Agreement shall be interpreted in a complementary manner to the extent possible.
    2. For all matters related to personal data protection and mandatory compliance with the Personal Data Protection Law and its Regulations, this Addendum shall prevail **only to the extent strictly necessary** to achieve such compliance.
    3. Otherwise, and in the event of any actual conflict between this Addendum and the Master Agreement, the provisions of the Master Agreement shall prevail, and no clause in this Addendum shall be interpreted in a way that diminishes or restricts any rights, limitations of liability, ownership rights, or powers granted to the First Party under the Master Agreement.
    4. In the event of conflict between this Addendum and any Standard Contractual Clauses stated in **Annex (2)** in relation to cross-border transfers of personal data, the Standard Contractual Clauses shall prevail **only to the extent required** to legitimize the transfer under Applicable Law.

Article (2): Parties and Their Roles in Data Protection

1. The Parties acknowledge that:
    - The **Second Party** is the **Data Controller** in relation to the personal data processed on the basis of the Master Agreement;
    - The **First Party** is the **Data Processor** in relation to such data, and only to the extent necessary to perform the Revenue Cycle Management services and related services pursuant to the Master Agreement and this Addendum.
2. The Second Party remains responsible for:
    - Determining the purposes and means of processing personal data;
    - Complying with its obligations to provide all required notices to Data Subjects and obtain any legally required consents from them, where applicable, in accordance with the PDPL;
    - Ensuring that its written instructions to the First Party are lawful, accurate, and do not conflict with Applicable Law or Regulations.
3. The Second Party acknowledges that the quality of services provided by the First Party depends on the Second Party's compliance with providing accurate, complete, and timely data, in accordance with the Master Agreement, particularly Articles (4) and (15) thereof.
4. Without prejudice to the above and without limiting the rights of the First Party under the Master Agreement, particularly Article (8/4):
   The First Party retains the right to use, process, and transform data into aggregated or anonymized data that can no longer identify any natural person, and to exploit such data (including selling, licensing, or sharing it) provided that such processing is compliant with the PDPL and does not result in the disclosure of any personal data. This is in line with the detailed provisions of the Master Agreement.

Article (3): First Party Obligations (Data Processor) in Processing Personal Data

Without prejudice to the Master Agreement, the First Party undertakes to:

1. Process personal data only to the extent required for the Business Purposes and for the performance of the services specified in the Master Agreement, and on the basis of written instructions from the Second Party, and within the limits permitted by law.
2. Refrain from using personal data for any purpose independent from the performance of the services, except in connection with transforming such data into aggregated or anonymized data and dealing with it in accordance with Article (2/4) above and Article (8/4) of the Master Agreement.
3. Inform the Second Party without undue delay if it considers that any of the Second Party's instructions regarding processing may conflict with the PDPL or its Regulations.
4. To the extent reasonably possible and based on the information available to it, assist the Second Party in fulfilling its legal obligations with respect to:
    - Data Subject rights (access, rectification, deletion, restriction of processing, objection, data portability, etc.);
    - Conducting Data Protection Impact Assessments where required;
    - Communicating with relevant regulatory authorities, all within realistic and reasonable limits and without imposing any additional obligations on the First Party beyond those set out in the Master Agreement or this Addendum.
5. Maintain the confidentiality of personal data and not disclose it except:
    - To employees, contractors, or sub-processors whose work requires access to such data, provided they are bound by appropriate confidentiality obligations; or
    - Where disclosure is required under mandatory law or pursuant to an order from a competent court or regulatory authority, in which case the First Party shall notify the Second Party where legally permissible.

Article (4): First Party's Staff

The First Party undertakes to:

1. Ensure that any employee or collaborator who has access to personal data is bound by professional confidentiality obligations, whether under an employment contract, confidentiality agreement, or binding internal policies.
2. Ensure that staff involved in personal data processing receive appropriate training — in accordance with the First Party's policies — on personal data protection requirements, to the extent relevant to their roles.
3. Guide and instruct staff and relevant personnel regarding their obligations to protect personal data under the PDPL, this Addendum, and the Master Agreement.

Article (5): Data Security and Protection

1. The First Party shall implement appropriate technical and organizational measures to protect personal data against:
    - Unauthorized access, use, modification, or disclosure;
    - Accidental or unlawful loss, damage, or destruction.

    Such measures shall be as described in **Annex (3): Technical and Organizational Security Measures**.

2. These measures shall take into account the level of risk associated with the nature and sensitivity of the personal data and may include, without limitation:
    - mandatory encryption of Personal Data both in transit and at rest, whenever such data is of a sensitive nature – including health data – and in accordance with the requirements of the PDPL and its Executive Regulations;
    - Access control and authorization mechanisms;
    - Data backup and recovery measures;
    - System access monitoring;
    - Periodic testing and assessment of control effectiveness.
3. Nothing in this Article shall be interpreted as a commitment to absolute security or strict liability for any security incident. Liability shall be assessed in accordance with the agreed limitations of liability under the Master Agreement, particularly Article (15/6).

Article (6): Personal Data Breach

1. The First Party shall notify the Second Party immediately upon becoming aware of any of the following events related to the Personal Data subject to this Appendix:
2. Loss, damage, destruction, or substantial corruption of Personal Data;
3. Any unauthorized or unlawful Processing;
4. Any incident constituting a Personal Data Breach as defined under the Personal Data Protection Law.
5. The notification shall include, to the extent reasonably possible:
    - A description of the nature of the incident, the categories of data affected, and an approximate number of records impacted;
    - Potential impacts or consequences;
    - Corrective or preventive measures taken or proposed.
6. The First Party shall cooperate with the Second Party – within reasonable limits – to investigate the incident and mitigate its effects, without incurring any additional obligations beyond the limitations of liability stipulated in the Master Agreement and in this Addendum.

7. The Second Party retains the right to determine whether Data Subjects or regulatory authorities must be notified in accordance with Applicable Law, it being understood that such notification obligations fall primarily on the Controller (the Second Party).

Article (7): Cross-Border Transfers

1. The First Party undertakes not to transfer Personal Data outside the Kingdom of Saudi Arabia except in accordance with the requirements set forth in the Personal Data Protection Law (PDPL), its Executive Regulations, and the cross-border transfer regulations, and only to the extent necessary for performing the Services, operating systems, backups, or other legitimate purposes related to the Main Agreement. No actual transfer of Personal Data outside the Kingdom shall be carried out by the First Party except based on documented approval from the Second Party, whether such approval is included in this Appendix or provided through written instructions or official correspondence between the Parties, without prejudice to the obligations stipulated in the PDPL and its related regulations.
2. The Second Party hereby grants a general prior approval for the First Party to engage third-party service providers and Sub-processors, whether within or outside the Kingdom, whenever necessary or appropriate for the performance of the Services under the Agreement, provided that such Sub-processors are bound by data protection obligations that are no less protective than those set out in this Appendix and applicable laws, and that they are contractually bound to the essential obligations imposed on the First Party insofar as they relate to the Processing of Personal Data. The First Party shall notify the Second Party when a new category of Sub-processors is added, where practical.
3. In the event that Personal Data is transferred or hosted outside the Kingdom, the First Party shall ensure that an adequate level of legal protection is applied in accordance with the requirements of the PDPL and cross-border transfer regulations, including compliance with the instructions issued by SDAIA and other competent authorities. The First Party shall also ensure that any external party engaged in such processing or hosting is contractually bound to obligations that are substantially equivalent to those contained in this Appendix and in the Main Agreement, insofar as they relate to the protection of Personal Data.
4. The First Party shall be entitled — without the need for specific prior approval each time — to:
    - Enter into written contracts with sub-processors that include appropriate data protection obligations;
    - Use legally recognized cross-border transfer mechanisms (such as Standard Contractual Clauses or adequacy decisions) where required.
5. Where practicable, the First Party may, upon the Second Party's written request, provide a general overview of the main categories of sub-processors or system hosting locations, without prejudicing the confidentiality of the First Party's arrangements with its service providers or its business secrets.
6. The First Party remains responsible for selecting sub-processors in good faith and in compliance with Applicable Law, while any financial or legal liability shall remain subject to the limitations set out in Article (15/6) of the Master Agreement.

Article (8): Complaints and Data Subject Rights

1. The First Party shall, to the extent reasonably possible and based on the information and capabilities available to it, assist the Second Party when it receives Data Subject requests (such as requests for access, rectification, deletion, restriction of processing, or data portability), to the extent necessary and proportionate to the nature of the services.
2. If the First Party receives a request directly from a Data Subject relating to the exercise of any of their statutory rights, the First Party shall, where reasonably possible, refer the request to the Second Party, in its capacity as the Controller responsible for providing the formal response.
3. The First Party shall not be obliged to respond directly to Data Subjects regarding such requests unless this is expressly agreed in writing or explicitly required by Applicable Law.

Article (9): Term of the Addendum and Relation to the Master Agreement

1. This Addendum shall remain in force for the duration of the Master Agreement and any renewal thereof, and shall continue to apply for as long as the First Party retains any personal data subject to this Addendum under the Master Agreement, to the extent permitted by law.
2. The expiry or termination of the Master Agreement shall not relieve either Party from its obligations relating to confidentiality and personal data protection, which shall continue to apply for as long as any data remains in the possession or under the control of either Party, in accordance with Article (8/7) of the Master Agreement.

Article (10): Return or Deletion of Personal Data upon Termination

Without prejudice to the provisions of the Master Agreement, particularly those relating to accounts receivable, collections, and the continuation of certain obligations after termination, the following shall apply:

1. The Second Party may, within a reasonable period after termination of the Master Agreement, request a copy of the personal data processed on its behalf, to the extent technically and operationally feasible and in a format determined by the First Party.
2. Subject to the following paragraph, the First Party shall delete, destroy, or anonymize personal data subject to this Addendum within a reasonable period after the end of the contractual relationship, and in accordance with the Second Party's documented instructions where provided, to the extent such instructions do not conflict with the First Party's legal or contractual obligations or its statutory rights to defend itself or establish its rights."
3. The First Party may retain certain data or records containing personal data in the following cases:
    - Where retention is required under mandatory law or regulatory instructions;
    - Where retention is necessary to establish or defend a legal right or claim, or in relation to an existing or anticipated dispute;

- Where the data has been transformed into aggregated or anonymized data in accordance with Article (2/4) of this Addendum and Article (8/4) of the Master Agreement.

4. The deletion or return of personal data shall not result in the waiver or reduction of any financial entitlements of the First Party, nor of any of its obligations or other rights under the Master Agreement.

Article (11): Audit and Documentation

1. The First Party shall keep appropriate records of the personal data processing activities it carries out on behalf of the Second Party, to the extent required by the PDPL and its Regulations.
2. Where the Second Party — particularly in the context of statutory or regulatory requirements — requests general information about the security measures applied by the First Party, the First Party may provide summarized documents or reports (such as certifications or summary security audit reports), without compromising its trade secrets or disclosing sensitive details about its systems or infrastructure.
3. The Second Party may, where there are regulatory or legal requirements, request reasonable information or documentation evidencing the First Party's compliance with data protection requirements, including through remote assessments or documentation-based reviews, without prejudice to the First Party's information security or trade secrets. Onsite audits shall not be conducted unless expressly agreed in writing by the First Party, including agreement on scope and procedures, and provided that such audits do not conflict with the First Party's security policies or third-party confidentiality obligations.

Article (12): Intellectual Property and Aggregated Data

1. This Addendum does not result in any transfer of ownership of systems, platforms, software, dashboards, analytical tools, or reports provided by the First Party. All such rights remain the exclusive property of the First Party in accordance with Article (8/8) of the Master Agreement.
2. The Second Party expressly acknowledges the First Party's right to use and process data and to transform it into statistical, aggregated, or anonymized data, and to exploit such data commercially or technically, provided that such data is no longer attributable to an identified or identifiable natural person, and provided that such processing is carried out in accordance with the PDPL and applicable Regulations.

Article (13): Limitation of Liability and Indemnity

1. This Addendum does not create any additional indemnity obligations on the First Party beyond those expressly set out in the Master Agreement.

2. Any financial or legal liability arising from this Addendum — including liability relating to personal data processing — shall be subject to the same limitations of liability agreed under the Master Agreement, particularly Article (15/6), and such limitations may not be exceeded except to the extent explicitly required by Applicable Law.
3. Each Party remains responsible for its own compliance with applicable laws within its respective role (Controller or Processor), and only to the extent that a causal link exists between its act or omission and the alleged damage, subject to the provisions of the Master Agreement.

Article (14): Governing Law and Jurisdiction

1. The provisions of this Addendum, where not otherwise specifically addressed, shall be subject to the Master Agreement and to the laws and regulations in force in the Kingdom of Saudi Arabia relating to data protection, in particular the Personal Data Protection Law and its Implementing Regulations.
2. Jurisdiction over any dispute arising from the interpretation or application of this Addendum shall lie with the competent court in Riyadh, in accordance with Article (12) of the Master Agreement.

Article (15): Final Provisions

1. This Appendix (E) forms an integral part of the Master Agreement and shall be effective from the date of signature by both Parties, or from the effective date of the Master Agreement — whichever is later — unless otherwise agreed in writing.
2. In the event of any conflict between this Addendum and the Master Agreement, the Master Agreement shall prevail, **except** where a provision of this Addendum is strictly required to ensure mandatory compliance with the Personal Data Protection Law and its related Regulations.
3. No amendment to this Addendum shall be valid or binding unless made in writing and signed by both Parties.
4. This Addendum has been executed in two (2) original copies, each Party holding one copy. The First Party may issue electronic or digital copies thereof, which shall be legally valid, consistent with Article (21) of the Master Agreement.

Annex (1) – Personal Data Processing Purposes and Parameters

This Annex forms part of the Data Processing Addendum – Appendix (E) – and is used to define the specific processing activities carried out by the First Party on behalf of the Second Party.

1. Subject Matter of Processing

Provision of Revenue Cycle Management (RCM) services and related technical, operational, and analytical services, including:

- Medical and technical auditing of claims;
- Preparation and submission of claims to insurance companies and Third-Party Administrators (TPAs);
- Collection management and financial reconciliation;
- Eligibility and medical approvals management;
- Pharmacy Benefit Management (PBM);
- Reporting, dashboards, and analytics.

2. Duration of Processing

- For the entire duration of the Master Agreement and any renewal thereof;
- With certain processing or data retention continuing thereafter to the extent permitted by law, in accordance with Article (10) of this Addendum and the Master Agreement.

3. Purpose of Processing and Business Purposes

To enable the Second Party to:

- Effectively manage its revenue cycle (claims, collections, financial reconciliation);
- Improve the quality of medical and technical submissions and reduce denial rates;
- Manage approvals and eligibility electronically;
- Manage prescriptions and pharmacy benefits;
- Obtain financial, operational, and analytical reports to support decision-making.

Processing includes, without limitation:

- Collecting and receiving data from the Second Party's systems or integration platforms;
- Storing and organizing data in the First Party's systems;
- Using data in daily operational processing (auditing, claims, collections);
- Generating reports and dashboards based on the data;
- Transforming data into aggregated or anonymized data for statistical or commercial analysis, in compliance with Article (2/4) of this Addendum and the Master Agreement.

4. Categories of Personal Data

a. Patient and Beneficiary Data:

- Full/partial name;
- National ID/Iqama number/medical record number;
- Contact details (phone, email – where available);
- Insurance details (insurer, policy number, coverage class, membership ID);
- Claims data (diagnoses, medical services provided, medical codes, date of service, amounts, co-payments);
- Medical approvals data (eligibility checks, outcomes, approvals/denials).

b. Data relating to employees or staff of the Second Party involved in service delivery (where applicable):

- Name and job title;
- Professional contact details;
- Account credentials and access profiles granted for system use.

c. Financial data related to claims:

- Claim and payment amounts;
- Transfer dates;
- Payment notification and reconciliation references.

5. Categories of Data Subjects

- Patients and beneficiaries of the Second Party's healthcare services;
- Insured persons covered by insurance companies contracted with the Second Party;
- Employees and staff of the Second Party involved in service delivery (physicians, administrators, claims, finance, and IT staff);
- Representatives of insurance companies or TPAs to the extent their professional details are stored in the First Party's systems (e.g., business contact details).

6. Authorized Persons to Issue Instructions

- Those designated by the Second Party as authorized signatories or contact persons for data and operations under the Master Agreement;
- Any other person formally designated by the Second Party in writing or via agreed official communication channels between the Parties.

7. Processing of Data Outside the Kingdom and Legal Mechanism (if applicable)

If any data is transferred or hosted outside the Kingdom in the context of providing the services, such transfer/hosting shall:

- Comply with the PDPL and the Regulations on cross-border transfer of personal data; and
- Be based on one of the legally recognized mechanisms, such as:
    - Hosting in a country that the Competent Authority has determined to provide an adequate level of protection; or
    - Application of Standard Contractual Clauses (SCCs) with the external service provider; or
    - Any other mechanism approved in the future by SDAIA/NDMO.

Annex (2) – Cross-Border Transfers and Standard Contractual Clauses

1. General Principle

- As a general rule, personal data should be processed within the Kingdom as far as reasonably possible.
- Personal data shall not be transferred or made accessible outside the Kingdom except in cases permitted by Applicable Law and Regulations, and only to the extent necessary to provide the services, operate systems, perform backups, or provide technical support.

2. Basis and Conditions for Transfer

When personal data is transferred outside the Kingdom, the First Party shall:

1. Ensure that the transfer is made to a country or entity that provides an adequate level of data protection, as determined by the Competent Authority; or
2. Apply one of the permitted legal frameworks for cross-border transfers, such as:
    - Standard Contractual Clauses (SCCs) approved or recognized by SDAIA, where applicable;
    - Binding Corporate Rules (BCRs), where available;
    - Any other mechanism approved by the Competent Authorities.

3. Standard Contractual Clauses (SCCs)

- Where it is necessary to apply SCCs for the transfer of personal data, the First Party may — with the Second Party's authorization — enter into such clauses with external service providers involved in the hosting or transfer of data, in alignment with models approved by the Competent Authorities.
- Once executed, such SCCs shall be deemed a complementary part of this Addendum and may be maintained or referenced in separate agreements (such as service level agreements or hosting agreements).

4. Documentation of External Parties (if any)

The First Party may, upon the Second Party's request and to an appropriate extent, provide general information about categories of external service providers or hosting regions involved in cross-border data transfers, without compromising the confidentiality of the First Party's contracts or business secrets.

Annex (3) — Technical and Organizational Security Measures

1. Physical Access Controls

- Protecting data centers and offices that host systems or storage media containing personal data through measures such as:
    - Access card systems, biometrics, or other authentication means;
    - CCTV in sensitive areas;
    - Restricting physical access to authorized teams only.

2. System Access Controls

- Managing user accounts and privileges in line with the "least privilege" principle;
- Using strong passwords and, where appropriate, multi-factor authentication;

- Revoking or adjusting user rights when roles change or upon termination of the relationship with the First Party.

3. Data Access Controls

- Restricting access to personal data to employees or contractors whose job functions require such access;
- Logging and monitoring access to sensitive records;
- Applying "need-to-know" policies for data access.

4. Data Transmission Controls

- Using secure communication protocols (such as HTTPS/VPN) when exchanging data with the Second Party or related entities;
- Encrypting data in transit where technically and practically appropriate;
- Documenting and securing technical integration interfaces (APIs / integrations).

5. Input and Processing Controls

- Tracking key operations (such as creation, modification, or deletion of sensitive records) through audit logs;
- Validating input data, to the extent possible, to reduce errors;
- Implementing authorization/review controls for high-impact transactions (such as financial operations).

6. Backups and Business Continuity

- Implementing periodic backup mechanisms for critical data and systems;
- Testing data recovery and business continuity plans periodically where possible;
- Storing backup copies in secure locations.

7. Data Segregation

- Logically or permission-based segregation of client data from other clients' data according to the system design;
- When using test or development environments, using anonymized or masked data where possible, or applying measures that protect data against unauthorized access.

8. Vulnerability and Patch Management

- Regularly updating systems and applications to address known security vulnerabilities;
- Conducting vulnerability scans periodically where appropriate;
- Maintaining documented patch and vulnerability management procedures.