سياسة الخصوصية

مقدمة

نحن، شركة التأمين العربية ش.م.ل، نوضح لكم من خلال سياسة الخصوصية هذه كيفية حماية خصوصية حقوق العملاء وإحترامها، حيث نلتزم بمعاملة معلوماتكم بمسؤولية.

توضح هذه السياسة كيفية قيام شركة التأمين العربية بجمع واستخدام ومشاركة المعلومات عنكم أو منكم.

جمع معلوماتكم الشخصية

نحن، شركة التأمين العربية، نجمع المعلومات الشخصية عنكم من مصادر مختلفة . على سبيل المثال، نقوم بجمع المعلومات التي تقدمونها لنا من خلال الطلبات والنماذج .

كما نتعاقد مع شركاء أعمال مستقلين يساعدوننا في تقديم المنتجات والخدمات عبر الإنترنت أو عن طريق وسطاء الضمان أو مقدمي الخدمات الخارجيين الذين قد يحتفظون بالمعلومات التي تقدمونها.

يجوز لشركة التأمين العربية أيضًا جمع المعلومات التي تقدمها عند:

- تقديم طلب للحصول على معلومات من أحد المواقع الإلكترونية الخاصة بشركة التأمين العربية.
- استخدام الأدوات والحاسبات الإلكترونية المتاحة عبر الإنترنت.
- التقدم بطلب إلكتروني للحصول على المنتجات.
- الاشتراك في الخدمات الإلكترونية.
- إكمال نموذج إلكتروني عبر الإنترنت.
- إجراء المعاملات المالية أو التجارية عبر الوسائل الإلكترونية.

استخدام معلوماتكم الشخصية

تقوم شركة التأمين العربية بجمع المعلومات الشخصية والسرية أثناء ممارسة أعمالها العادية لتقديم الخدمات للعملاء .

وقد يتم استخدام هذه المعلومات للأغراض التالية:

1. التواصل معكم؛
2. معالجة طلباتكم وضمان دقة علاقتنا معكم؛
3. الرد على استفساراتكم؛
4. إرسال معلومات مهمة تتعلق بعلاقتكم مع شركة التأمين العربية، أو أي تغييرات على سياسة الخصوصية، أو أي أمور إدارية أخرى؛
5. السماح لكم بالمشاركة في الاستبيانات والعروض الترويجية؛

6. تحليل البيانات وإجراء التدقيق، وتطوير وتحسين المنتجات والخدمات الخاصة بالشركة والموقع الإلكتروني؛
7. تحديد اتجاهات الاستخدام وقياس فعالية الحملات الترويجية؛
8. الرقابة على المخاطر، والكشف عن الاحتيال ومنعه؛
9. الامتثال للأحكام وللقوانين المطبقة ؛
10. إرسال الاتصالات التسويقية التي قد تكون محل اهتمامكم.
11. في حال شرائك منتج مالي أو تأميني آخر، يجوز لنا مشاركة معلوماتك لأغراض تسويقية، وذلك وفقًا للأنظمة والقوانين المعمول بها.

مشاركة معلوماتكم الشخصية

قد نشارك معلوماتكم الشخصية مع معيدي التأمين، مقدمي الخدمات، والأطراف الثالثة التي تقوم بتقديم الخدمات والتسويق نيابة عنا .

وقد نقوم بمشاركة معلوماتكم كليًا أو جزئيًا وفقاً لما يقتضيه القانون أو المسموح به لأغراض قانونية أو تنظيمية أو لمكافحة الاحتيال.

تشمل هذه المعلومات التالي:

- يجوز لنا مشاركة المعلومات التي نتلقاها منك من خلال الطلبات أو النماذج الأخرى، والتي قد تتضمن اسمك، عنوانك، المستفيدين، رقم الضمان الاجتماعي، ومعلومات عن أفراد العائلة. وقد تشمل أيضًا بيانات الأصول، الدخل، عنوان العقار وقيمته.
- يجوز لنا مشاركة المعلومات المتعلقة بمعاملاتك مع شركاتنا الشقيقة، والتي قد تتضمن رصيد حسابك، التغطية التي توفرها لك الوثيقة، وسجل المدفوعات. كما قد تشمل الأقساط المدفوعة، التفضيلات، المطالبات، وطريقة الشراء.
- يجوز لنا مشاركة المعلومات التي نتلقاها من وكالات التقارير الاستهلاكية أو تقارير أخرى، والتي قد تشمل تقرير الائتمان الخاص بك، بيانات المركبة والسائق. وقد تتضمن أيضًا البيانات الطبية، بيانات التوظيف، تقارير سجل الخسائر، وغيرها من بيانات السائق.
- يجوز لنا مشاركة المعلومات المتعلقة بطريقة الدفع الخاصة بك مع الأطراف الثالثة المعتمدة. ولن يتم تخزين أو بيع أو مشاركة أو تأجير أي تفاصيل تتعلق ببطاقات الائتمان أو أي معلومات شخصية مُعرِّفة للهوية مع أي أطراف غير مصرح لها.

يمكنك العثور على رابط لبعض الجهات التي يُسمح لها بالوصول إلى جزء أو كل معلوماتك السرية لأغراض تجارية من قبل شركة التأمين العربية:

- R+V Versicherung AG

فيما يتعلق بمعالجة بياناتك الشخصية وفقًا لتعريف اللائحة العامة لحماية البيانات الأوروبية (GDPR) من قبل شركائنا الأوروبيين، يمكنك العثور على مزيد من المعلومات حول الشركات المعنية، وفقًا للمادة 14 من اللائحة العامة لحماية البيانات، عبر الرابط التالي:

لمزيد من المعلومات حولR+V Versicherung AG ، يُرجى زيارة الرابط التالي:

http://www.gdpr.ruv.de

استخدام معلوماتكم الطبية

قد نضطر أحيانًا إلى جمع معلومات طبية لتقديم منتج أو لدفع مطالبة .

يتم استخدام المعلومات الطبية عند:

- الاكتتاب؛
- تقديم الخدمات المتعلقة بالوثيقة أو الحساب أو المطالبة؛
- كما هو مطلوب أو مسموح به بموجب القانون؛
- بناءً على طلبكم وبموافقتكم.

دقة المعلومات

يجب أن تكون المعلومات الشخصية والحساسة دقيقة وكاملة ومحدثة بقدر ما هو ضروري لغرض استخدامها. في حال كنت تعتقد أن معلوماتك غير دقيقة أو غير مكتملة أو غير محدثة، يُرجى التواصل مع شركة التأمين العربية أو مع وكيلك المعتمد لاتخاذ الإجراءات اللازمة.

الأمان والسرية

تتم حماية المعلومات الشخصية والسرية من خلال تدابير أمنية تتناسب مع درجة حساسية المعلومات. وتشمل هذه التدابير وسائل الحماية ضد الفقدان، أو السرقة، أو الإطلاع غير المصرح به، أو النسخ، أو الاستخدام، أو التعديل، وذلك من خلال:

التدابير الأمنية المادية: مثل الأقفال، والمناطق ذات الوصول المقيد، وغيرها.

التدابير التنظيمية: مثل تصاريح الأمان، وعمليات التفويض والموافقة.

التدابير التكنولوجية: مثل كلمات المرور، والتشفير، والمصادقة متعددة العوامل.

يتم تصميم هذه التدابير الأمنية وفقًا لمستوى حساسية المعلومات لضمان أعلى درجات الحماية.

نستخدم إجراءات وقائية مادية وتقنية لحماية معلوماتك، كما نحد من الوصول إليها ليقتصر فقط على الموظفين الذين يحتاجون للاطلاع عليها من أجل تنفيذ مهامهم. كما أن شركاء الأعمال الأطراف الثالثة ملزمون قانونًا باستخدام المعلومات حصريا لأغراضنا المحددة، ولا يجوز لهم الإفصاح عنها أو استخدامها بأي شكل آخر. نحن ملتزمون بالامتثال والتقيد بجميع القوانين واللوائح المتعلقة بحماية البيانات.

تعديلات وتغييرات سياسة الخصوصية

إن هذه السياسة قابلة للتعديل دون أي إشعار مسبق، وستصبح التغييرات المنشورة على الموقع سارية المفعول فورًا.

لذلك، ننصح العملاء بزيارة هذه الأقسام بشكل متكرر للبقاء على اطلاع على أحدث التعديلات.

الموقع الإلكتروني ووسائل التواصل الاجتماعي

سياسة الخصوصية

يجوز لشركة التأمين العربية جمع معلومات لا تكشف عن هويتك بشكل صريح أو لا ترتبط مباشرة بشخص معين، مثل المعلومات التي يتم جمعها من خلال ملفات تعريف الارتباط(Cookies) ، بيانات المتصفح، التقنيات الأخرى، المعلومات الديموغرافية، وأي معلومات أخرى تقدمها.

كما يجوز لشركة التأمين العربية جمع واستخدام هذه المعلومات بطرق متعددة، تشمل – على سبيل المثال لا الحصر – ما يلي:

- بيانات المتصفح
- ملفات تعريف الارتباط(Cookies)
- عنوان بروتوكول الإنترنت(IP Address)
- البيانات المجمّعة

تقوم شركة التأمين العربية أو شركاؤها التجاريون باستخدام المعلومات التي يتم جمعها من مواقعها الإلكترونية للأغراض التالية:

- إجراء التعديلات وتلقي الملاحظات
- التسويق والعروض الترويجية
- تحليل سلوك المستخدم

- تطوير المنتجات
- تحسين المحتوى
- إبلاغ المعلنين بعدد الزوار الذين شاهدوا أو نقروا على إعلاناتهم
- تخصيص محتوى الموقع الإلكتروني وتخطيطه وفقًا لاحتياجات المستخدمين

الإعلانات

يجوز لشركة التأمين العربية عرض إعلانات على موقعها الإلكتروني وكذلك على المواقع الإلكترونية التابعة لها. تشمل المعلومات التي يتم جمعها من قبل شركة التأمين العربية أو مزودي خدمات الإعلانات من خلال ملفات تعريف الارتباط (Cookies) والتقنيات الأخرى، بيانات حول عدد الأشخاص الذين يتصفحون الموقع، وأنماط التصفح داخل الموقع، ومدى تفاعل المستخدمين مع الإعلانات والعروض الترويجية سواء على الموقع أو على مواقع إلكترونية أخرى حيث تقوم الشركة بالإعلان.

يجوز لشركة التأمين العربية الترويج لمنتجاتها وخدماتها على هذا الموقع، بما في ذلك العروض المتعلقة بوثائق التأمين. وقد تأخذ هذه الإعلانات أشكالًا متعددة، مثل:

- الإعلانات المنبثقة (Splash Ads) التي تظهر عند تسجيل الدخول أو الخروج من الحسابات الإلكترونية.
- إعلانات البانر (Banner Ads) وغيرها من الأشكال الإعلانية الرقمية.

كما تستعين شركة التأمين العربية بمزودي خدمات الإعلانات لتحديد الإعلانات التي من المرجح أن تهمك، وذلك باستخدام بيانات مثل:

- الصفحات التي تمت زيارتها.
- الكلمات المفتاح التي تم البحث عنها.
- أنشطتك على الموقع الإلكتروني.

تقوم شركة التأمين العربية بتقييد الوصول إلى المعلومات وجمعها لأغراض محددة فقط لصالح مزودي خدمات الإعلانات.

مواقع الأطراف الثالثة

قد توفر شركة التأمين العربية روابط لمواقع إلكترونية تابعة لأطراف ثالثة، مثل شركات إعادة التأمين أو مقدمي الخدمات. في حال قمت بمتابعة هذه الروابط والوصول إلى مواقع لا تخضع لإدارة أو سيطرة شركة التأمين العربية، يتعين عليك مراجعة سياسات الخصوصية والسرية، وكذلك الشروط والأحكام الخاصة بتلك المواقع، حيث قد تختلف عن تلك المعتمدة لدى شركة التأمين العربية.

لا تتحمل شركة التأمين العربية أي مسؤولية عن سرية أو خصوصية هذه المواقع، بما في ذلك مدى اكتمال المعلومات، أو دقتها، أو موثوقيتها، كما أنها لا تضمن حماية البيانات التي يتم تبادلها عبر هذه المواقع.

قد يتم عرض بعض الإعلانات على هذا الموقع الإلكتروني من قبل أطراف ثالثة، مثل شبكات الإعلانات، ووكالات التسويق، والمعلنين، ومزودي تحليل الجمهور. قد تقوم هذه الأطراف بجمع معلومات حولك وحول نشاطك على الإنترنت، سواء على هذا الموقع أو مواقع أخرى، وذلك باستخدام ملفات تعريف الارتباط(Cookies) ، وإشارات الويب (Web Beacons)، وتقنيات أخرى، بهدف فهم اهتماماتك وتقديم إعلانات مخصصة لك.

يرجى أخذ العلم بأن شركة التأمين العربية لا تمتلك حق الوصول إلى هذه المعلومات التي تجمعها الأطراف الثالثة، أو السيطرة عليها. كما أن ممارسات جمع البيانات الخاصة بهذه الأطراف الثالثة لا تخضع لأحكام سياسة الخصوصية الخاصة بشركة التأمين العربية.

وسائل التواصل الاجتماعي

قد تستخدم شركة التأمين العربية منصات التواصل الاجتماعي، بما في ذلك على سبيل المثال لا الحصر، فيسبوك (Facebook)، تويتر (Twitter) ، ولينكدإن(LinkedIn) ، وذلك لتمكين المستخدمين من التفاعل والتواصل معها عبر الإنترنت.

أي محتوى تقوم بنشره على الصفحات الرسمية لشركة التأمين العربية على وسائل التواصل الاجتماعي، بما في ذلك الآراء، الصور، أو أي معلومات شخصية أخرى تتيحها للمشاركين على هذه المنصات، يخضع لشروط الاستخدام وسياسات الخصوصية الخاصة بتلك المنصات.

لذا، يُنصح بمراجعة السياسات الخاصة بتلك المنصات لفهم حقوقك والتزاماتك المتعلقة بالمحتوى الذي تشاركه عل هذه المنصات . بالإضافة إلى ذلك، يرجى ملاحظة أنه عند زيارة أي من الصفحات الرسمية لشركة التأمين العربية على وسائل التواصل الاجتماعي، فإنك تخضع أيضًا لسياسة الخصوصية الخاصة بشركة التأمين العربية.

إخلاء المسؤولية والموافقة على استخدام منصة E-Arabia

إخلاء المسؤولية

من خلال الوصول إلى منصة E-Arabia ، أو تصفحها، أو استخدامها، أو تنزيل أي مواد منها، فإنك تقر بأنك قد قرأت هذه السياسة، وفهمتها، وتوافق على الالتزام التام بجميع الأحكام والشروط الواردة فيها دون أي قيود أو تحفظات، وتكون ملزمًا قانونيًا بها.

تنطبق هذه السياسة على استخدامك لمنصة E-Arabia بغض النظر عن الطريقة التي وصلت بها إلى المنصة. في حال عدم موافقتك على الالتزام القانوني بهذه السياسة، يجب عليك التوقف فورًا عن استخدام منصة E-Arabia ومغادرتها.

تحتفظ شركة التأمين العربية ("الشركة") بحقها المطلق في تعديل أو تغيير هذه السياسة في أي وقت دون إشعار مسبق. ويُعتبر استمرارك في استخدام منصة E-Arabia بعد نشر أي تعديلات عليها بمثابة قبولك الضمني للسياسة المعدلة. إذا قررت في أي وقت عدم قبول هذه السياسة، فأنت غير مخوّل باستخدام المنصة.

يحظر عليك استخدام منصة E-Arabia للقيام بأي أنشطة غير قانونية أو احتيالية، أو ممارسة أي تصرف تشهيري، أو مسيء، أو تهديدي، أو مضايقة، أو انتهاك لحقوق الملكية الفكرية أو أي حقوق ملكية أخرى خاصة بأطراف ثالثة. كما تخلي شركة التأمين العربية مسؤوليتها عن أي أفعال من هذا النوع، ولن تكون ملزمة بتقديم أي تغطية تأمينية أو الاستمرار بها للمستخدم المخالف.

إن جميع البيانات والتصريحات المتعلقة بالسياسات التأمينية والتغطيات المدرجة على منصة E-Arabia هي لأغراض المعلومات العامة فقط.

لا يمكن إتمام أو تعديل أو تغيير أي تغطية تأمينية من خلال تقديم أي نموذج أو طلب إلكتروني عبر المنصة، أو عبر البريد الإلكتروني، أو البريد الصوتي، أو الفاكس. ولا تصبح أي وثيقة تأمين، أو تعديل، أو إضافة، أو حذف سارية المفعول إلا بعد موافقة شركة التأمين العربية الرسمية والمباشرة.

أي عرض تأميني يتم تقديمه لك من خلال المنصة يعتمد على المعلومات التي تقدمها عبر النماذج الإلكترونية أو أي وسائل اتصال أخرى. ولا تكون شركة التأمين العربية ملزمة بتقديم التغطية التأمينية في حال تقديم معلومات خاطئة، أو مضللة، أو غير مكتملة، أو في حالة الاحتيال.

قد لا تكون بعض المنتجات والخدمات المدرجة على منصة E-Arabia مسجلة أو معتمدة من قبل البنك المركزي، أو الجهات الحكومية، أو الرقابية في بعض الدول التي تمارس فيها الشركة أعمالها، أو في الدولة التي يقيم فيها المستخدم.

وبالتالي، قد لا تتمتع بالحماية القانونية والتنظيمية التي توفرها قوانين بلد إقامتك فيما يتعلق بالمنتجات أو الخدمات التي يتم الإشارة إليها أو بيعها من خلال منصة E-Arabia.

حدود المسؤولية

في أي حال من الأحوال، لا تتحمل شركة التأمين العربية أو وكلاؤها أو موظفوها أي مسؤولية عن أي أضرار أو خسائر أو نفقات تنشأ نتيجة:

- استخدام منصة E-Arabia أو عدم القدرة على استخدامها من قبل أي طرف.
- أي أعمال احتيالية، أو فشل في الأداء، أو أخطاء، أو إغفال، أو انقطاع، أو عيوب.
- أي تأخير في التشغيل أو الإرسال، أو فيروسات حاسوبية، أو أعطال في الخطوط أو الأنظمة.

وذلك حتى في الحالات التي يتم فيها إبلاغ شركة التأمين العربية أو ممثليها مسبقًا بإمكانية وقوع مثل هذه الأضرار أو الخسائر أو النفقات.

بند العقوبات

لن تقبل شركة التأمين العربية أو بتسديد أي دفعة مالية، أو تنفيذ أي معاملة، أو تقديم أي خدمة أو منتج، إذا كان من شأن ذلك أن يعرض الشركة لأي عقوبة، أو غرامة، أو حظر، أو قيود بموجب:

- قرارات الأمم المتحدة.
- العقوبات التجارية أو الاقتصادية.
- القوانين أو اللوائح المعمول بها في الاتحاد الأوروبي، المملكة المتحدة، الولايات المتحدة الأمريكية، أو أي دول أخرى تؤثر على أعمال الشركة.
- القوانين أو اللوائح السارية في الدول التي تمارس فيها الشركة أنشطتها.
- ويظل امتثال الشركة لهذه الأحكام شرطًا أساسيًا في جميع تعاملاتها المالية والتجارية.

الموافقة

من خلال نقل المعلومات عبر منصةE-Arabia ، فإنك تمنح موافقتك على استخدامها، وتوافق على الالتزام بأي بيان، أو تأكيد، أو موافقة، أو اتفاق تقدمه أو ترسله عبر المنصة، بما في ذلك – على سبيل المثال لا الحصر – أي موافقة تمنحها لاستلام السجلات أو الاتصالات من شركة التأمين العربية من خلال الوسائل الإلكترونية فقط.

أنت تقر وتوافق على أن شركة التأمين العربية غير ملزمة بالتحقق من هوية أو سلطة أي مستخدم لهذا الموقع، كما أنك تتحمل المخاطر المرتبطة بنقل المعلومات إلينا أو تلقي المعلومات منا، والتي قد يتم اعتراضها من قبل أطراف ثالثة.

الاستفسارات

لمزيد من المعلومات، يرجى الاتصال بأقرب مكتب إقليمي لك عبر الرابط التالي:

https://www.arabiainsurance.com/en

شركة التأمين العربية

شركة التأمين العربية

ميثاق حماية البيانات والسرية

تم إصدار هذا المستند للمرة الأولى في أغسطس 2023، متضمناً المنهجية والبنية المقترحة. وتم توثيق أي تعديلات جوهرية أُجريت لاحقًا على هذا الإطار بوضوح، مع الإشارة إلى تاريخ إدخال كل تعديل.

الاختصارات

الاختصار	الوصف
AIC	شركة التأمين العربية
BOD / Board	الإدارة مجلس
BT	الأعمال تقنية
CBB	المركزي البحرين مصرف
CEO	التنفيذي الرئيس
AICالشركة /	والأجنبية المحلية وفروعها لبنان
CISO	المعلومات لأمن التنفيذي المسؤول
DHA	بدبي الصحة هيئة
DPO	البيانات حماية مسؤول
ERM	المؤسسات مخاطر إدارة
GDPR	البيانات لحماية الأوروبي النظام
HIA	الصحية المعلومات أصول
HIPAA	الصحية البيانات وحماية نقل قانون
ICT	والاتصالات المعلومات تكنولوجيا
IG	المعلومات حوكمة
ISMSC	المعلومات أمن إدارة نظام لجنة
IT	المعلومات تقنية
KPIs	الرئيسية الأداء مؤشرات
NESA	الإلكتروني للأمن الوطنية الهيئة
PHI	المحمية الصحية المعلومات
QCB	المركزي قطر مصرف
RCC	والامتثال المخاطر لجنة
SEM	التنفيذية الإدارة
SSL	الآمنة المقابس طبقة
UAE	المتحدة العربية الإمارات
URL	الصفحة مواقع محدد

المحتويات الأساسية

1. المقدمة 3
2. نطاق التطبيق 3
3. الإطار التنظيمي 4
4. الحوكمة والمسؤوليات 4
- الرئيس التنفيذي 4
- لجنة نظام إدارة أمن المعلومات(ISMSC) 5
- المسؤول التنفيذي لأمن المعلومات (CISO) 5
- مسؤول حماية المعلومات (DPO) 5-6
- مدير حوكمة المعلومات (IG MANAGER) 6
- المدراء المباشرون (LINE MANAGER) 6
- جميع الموظفين 6
5. إدارة المخاطر 7
6. مبادئ حماية البيانات والسرية 7
- المعلومات الصحية المحمية 8
- المعالجة 8
- موافقة صاحب البيانات 8
- أطراف ثالثة 8
- النقل و التخلص 8
- خرق حماية البيانات و السرية 9
- الاستجابة للحوادث و التبليغ 9
- حماية البيانات حسب التصميم و الإعداد الافتراضي 9
- حقوق صاحب البيانات على المعلومات الصحية المحمية 9
- أنظمة تكنولوجيا لامعلومات (IT) 9
- إدارة الأجهزة (الطبية و غير الطبية) 10
- إدارة وسائط التخزين القابلة للإزالة 10
- الأمن الفيزيائي و ضوابط الوصول PHI/HIA 10
- معالجة PHI من خلال منصة نبض (Nabidh HIE) 10
7. تصنيف أصول المعلومات الصحية HIA 10
8. إعادة تصنيف اصول المعلومات الصحية 10
9. وضع ملصقات على الأصول الصحية 10
10. تصاريح الوصول إلى الأصول الصحية داخل الشركة 10
11. إدارة أصول المعلومات الصحية 11
12. استخدام الحلول السحابية 11
13. رقمنة السجلات الطبية 11
14. استمرارية الأعمال/خطط التعافي من الكوارث 11
15. التدريب 11
16. إغلاق أو اندماج الشركة 11
17. المستثلة 11
18. المراقبة و الامتثال 11
19. عدم الامتثال 11
20. الملحقات 12
- الملحق – أ: الأقر المحتمل 12
- الملحق – ب: تصنيفات أصول المعلومات الصحية 12
- المحلق -ج: ضوابط الوصول إلى الأصول الصحية 12
- الملحق – د: متطلبات تخزين الأصول الصحية 12
- ملحق – هـ: متطلبات إعادة استخدام / إتلاف الأصول الصحية 12

I. المقدمة

في السنوات الأخيرة، أصبحت خصوصية البيانات محل اهتمام متزايد لدى جميع الشركات، لا سيما الجهات العاملة في القطاع الصحي .ويتعين على مقدمي الرعاية الصحية ضمان الإدارة السليمة لبيانات المرضى، بهدف تعزيز ثقافة الثقة والشفافية مع المرضى، إلى جانب الالتزام بالتشريعات الصارمة المتعلقة بحماية البيانات. تتطور خصوصية البيانات في مجال الرعاية الصحية بشكل مستمر، تماشيًا مع التحديثات المتلاحقة في القوانين واللوائح التنظيمية. وبصفتها شركة تأمين تعمل منذ أكثر من 75عامًا، ولها حضور في ثماني دول عربية، تقدم شركة العربية للتأمين ويُشار إليها لاحقًا بـ "العربية" أو(AIC) تغطية تأمينية صحية لعملائها، مما يضعها في موقع حساس من حيث التعامل مع معلومات شخصية حساسة. ونظرًا لأن المعلومات الصحية المحمية (PHI) تُعد من أكثر البيانات خصوصية بالنسبة للفرد – وذات قيمة عالية لدى المجرمين –فإن الإرشادات المنظمة لمقدمي الرعاية الصحية وغيرهم من الجهات التي تتعامل مع هذه المعلومات، أو تقوم باستخدامها أو نقلها، تتضمن متطلبات صارمة لحماية البيانات، بالإضافة إلى عقوبات مشددة في حال عدم الامتثال لتلك المتطلبات.

II. نطاق التطبيق

نطاق الإرشادات والإجراءات الواردة في هذا الميثاق على شركة العربية للتأمين في لبنان وجميع فروعها المحلية والأجنبية في مناطق العمليات التابعة لها، بما يشمل جميع الأنظمة والموظفين والأطراف الثالثة الذين لديهم إمكانية الوصول إلى أنظمتها .ولغرض الامتثال لأفضل الممارسات، يأخذ هذا الميثاق في الاعتبار جميع القواعد والإرشادات الصادرة عن الجهات التنظيمية في الدول التي تعمل بها فروع الشركة، بما في ذلك البحرين والكويت وقطر والإمارات العربية المتحدة.

III. الإطار التنظيمي

يستند هذا الميثاق إلى القوانين والمتطلبات التنظيمية الصادرة عن دولة الإمارات العربية المتحدة وإمارة دبي، بما في ذلك:

- القانون الاتحادي رقم (2) لسنة 2019 بشأن استخدام تكنولوجيا المعلومات والاتصالات في المجال الصح ولائحته التنفيذية.
- القرار رقم (2) لسنة 2017 بشأن اعتماد وثيقة سياسات تصنيف وتبادل وحماية البيانات في دبي.
- قرارات الهيئة العامة لتنظيم قطاع الاتصالات والحكومة الرقمية.(TDRA)
- القرار التنفيذي رقم (51) لسنة 2021 والمعروف بقانون تكنولوجيا المعلومات والاتصالات الصحي.
- القانون الاتحادي رقم (45) لسنة 2021 بشأن حماية البيانات.
- القرار الوزاري الاتحادي رقم 51 لسنة 2021 بشأن حالات السماح بتخزين ونقل البيانات الطبية خارج الدولة.
- سياسات هيئة الصحة بدبي لتصنيف أصول المعلومات الصحية.
- معايير الهيئة الوطنية للأمن الإلكتروني.(NESA)
- لائحة تنظيم أمن المعلومات لحكومة دبي.(ISR)
- نظام إدارة أمن المعلومات.ISO 27001 - (ISMS)
- القوانين الإماراتية الاتحادية والمحلية بشأن الأمن السيبراني.
- سياسات الهيئة مثل سياسات نبض، حماية وجودة وأمن البيانات الصحية.
- متطلبات مركز دبي للأمن الإلكتروني.
- متطلبات حكومة دبي الذكية.
- متطلبات مطالبات التأمين والتوثيق الصادرة عن هيئة الصحة بدبي.

IV. الحوكمة والمسؤوليات

V. الرئيس التنفيذي (CEO)

يتحمّل **الرئيس التنفيذي (CEO)** المسؤولية النهائية عن ضمان وجود ترتيبات مناسبة لإدارة حماية البيانات والسرية، من خلال سياسات تدعم تنفيذ واستخدام ومعالجة البيانات. يجب أن تضمن هذه السياسات أن تتم معالجة البيانات بشفافية وشرعية ودقة وأمان وعلى أساس قانوني، بما يتماشى مع مبادئ حماية البيانات والسرية، بما في ذلك المعلومات الصحية المحمية(PHI)

كما يتحمل الرئيس التنفيذي مسؤولية توفير الموارد الكافية لدعم متطلبات الميثاق ودور مسؤول حماية البيانات، بما في ذلك أنظمة تكنولوجيا المعلومات، والموظفين، والميزانية اللازمة، وغيرها.

لجنة نظام إدارة أمن المعلومات (ISMSC)

تمثل لجنة نظام إدارة أمن المعلومات (ISMSC) التزام الإدارة العليا بأمن المعلومات داخل شركة العربية. وتشمل مسؤوليات اللجنة ما يلي:

- مراجعة واعتماد ميثاق حماية البيانات والسرية.
- توفير الموارد اللازمة لتخطيط وتنفيذ ومراقبة وتحسين أمن المعلومات.
- التأكد من وجود ضوابط كافية ضمن أنظمة تكنولوجيا المعلومات لمنع فقدان البيانات أو معالجتها بشكل غير قانوني أو الوصول غير المصرح به إليها.
- ضمان أن الترتيبات مع الجهات الخارجية للوصول إلى الأنظمة تكون بناءً على اتفاق رسمي يحدد متطلبات الأمان.
- تقديم تقارير إلى لجنة المخاطر والامتثال (RCC) حول الأمور المتعلقة بالأمن، كحالات خرق البيانات، ونتائج التدقيق، والتقارير الدورية، وغيرها.

المسؤول التنفيذي لأمن المعلومات(CISO)

يرأس وظيفة إدارة أمن المعلومات، ويكون مسؤولاً عن:

- تقديم تقارير منتظمة إلى لجنة ISMS حول جميع الأمور المتعلقة بالأمن.
- توصيل سياسات أمن المعلومات إلى جميع الأطراف المعنية والعملاء عند الحاجة.
- مراقبة وتحليل الحوادث الأمنية وأثرها.
- وضع إجراءات لتوثيق وتصنيف وتصعيد وحل الحوادث الأمنية.
- تقديم برامج توعية وتدريب للموظفين كل سنتين لدعم الامتثال لهذا الميثاق.

مسؤول حماية البيانات(DPO)

يتطلب قانون حماية البيانات الإماراتي من جميع الكيانات والمُعالِجين للبيانات تعيين مسؤول حماية بيانات (DPO) يتمتع بالصفات المهنية والمعرفة الكافية بالامتثال لحماية البيانات. يمكن أن يكون DPO موظفًا داخل الشركة أو طرفًا خارجيًا يتم تعيينه. وستقوم شركة العربية بتعيين مدير الامتثال كجهة مسؤولة عن التحكم في البيانات، وستشارك بيانات الاتصال الخاصة بـ DPO مع مكتب المعلومات الإماراتي وهيئة الصحة بدبي.

تشمل مسؤوليات DPO ما يلي:

- الإشراف على تنفيذ تدابير حماية وأمن البيانات والامتثال للوائح ذات الصلة.
- ضمان شرعية ودقة عمليات حماية البيانات.
- استقبال ومعالجة جميع الشكاوى المتعلقة بحماية البيانات والسرية.
- تقديم المشورة الفنية حول تقييمات حماية البيانات، وإجراءات التفتيش الدورية، وأنظمة الحماية من الخروقات.
- توثيق جميع تقييمات حماية البيانات وإجراءات إدارة المخاطر.
- تقديم تقارير مباشرة إلى الرئيس التنفيذي ومجلس الإدارة.
- تقديم التوعية والتدريب حول القوانين واللوائح المتعلقة بحماية البيانات.
- تمثيل الشركة كنقطة اتصال رئيسية مع الجهات التنظيمية.
- الحفاظ على سرية البيانات وخاصة المعلومات الصحية المحمية.

مدير حوكمة المعلومات(IG Manager)

يكون مدير حوكمة المعلومات أو أي موظف مكلف بمهام مماثلة مسؤولاً عن فرض وتطبيق هذا الميثاق. ويجب على قسم حوكمة المعلومات دعم الأقسام المختلفة في تطبيق الضوابط المحددة وضمان الامتثال، وتقديم التوعية اللازمة للمستخدمين. يجب الإبلاغ عن أي خرق متعلق بأصول أو معلومات صحية محمية إلى قسم الحوكمة.

المدراء المباشرون(Line Managers)

يكون المدراء مسؤولين عن ضمان الامتثال لسياسات حماية البيانات داخل إداراتهم، والتأكد من أن جميع الموظفين الدائمين أو المؤقتين، والمقاولين، على دراية بـ:

- ميثاق حماية البيانات والسرية كما ينطبق على مجالات عملهم.
- مسؤولياتهم الفردية في التعامل مع المعلومات الصحية المحمية.
- متطلبات الإبلاغ والامتثال.
- كيفية وأماكن الحصول على المشورة عند التعامل مع البيانات.
- التأكد من أن جميع الموظفين أكملوا التدريب الإلزامي.

جميع الموظفين

يخضع جميع الموظفين العاملين في شركة العربية لقانون حماية البيانات الإماراتي، حيث أن لديهم:

- حقوق كموظفين يتم الاحتفاظ ببيانات عنهم من قبل الشركة.
- التزامات كمحترفين صحيين يجمعون بيانات عن الأشخاص الخاضعين للبيانات.
- **يجب على جميع الموظفين:**
  - فهم التزاماتهم القانونية في الحفاظ على سرية المعلومات الصحية المحمية.
  - المشاركة في تدريبات التوعية والتوجيه.
  - معرفة الجهات المسؤولة عن حماية البيانات داخل الشركة.
  - التحقق من هوية أي شخص يطلب بيانات سرية قبل الإفصاح عنها.
  - الإبلاغ عن أي خروقات فعلية أو مشتبه بها للسرية إلى مديرهم المباشر.
  - التوقيع على اتفاقيات السرية وعدم الإفشاء إن كانوا يتعاملون مع بيانات حساسة أو سرية.

إدارة المخاطر

تُعتبر إدارة المخاطر وظيفة رقابية، وهي مسؤولة عن وضع عملية شاملة لإدارة المخاطر بما يضمن تحديدها وقياسها ومراقبتها والإبلاغ عنها في الوقت المناسب، بما يشمل المخاطر التي قد تؤثر على أمن البيانات.

تشمل مسؤوليات إدارة المخاطر:

- مساعدة CISO في تطوير ميثاق حماية البيانات والسرية بما يتماشى مع اللوائح وأفضل الممارسات.
- ضمان امتثال شركة العربية للضوابط والإجراءات الواردة في هذا الميثاق.
- إبلاغ الإدارة بأي تغييرات أو تحديثات في الميثاق.
- تطوير ومراجعة السياسات الخاصة بأمن المعلومات ضمن إطار إدارة المخاطر المؤسسية.(ERM)
- التنسيق مع مختلف الإدارات مثل تكنولوجيا الأعمال والامتثال والشؤون القانونية بشأن تحديث أطر العمل المتعلقة بالأمن السيبراني وحماية البيانات.
- تقييم المخاطر المرتبطة بالإفصاح كما هو موضح في الملحق أ.

VI. مبادئ حماية البيانات والسرية

تلتزم شركة العربية بحماية وتأمين جميع أنواع المعلومات الشخصية (بما في ذلك الصحية) التي تجمعها من عملائها وموظفيها وغيرهم. وفيما يلي المبادئ الأساسية للتعامل مع هذه المعلومات:

- **العدالة والمشروعية والشفافية**
يجب أن يكون جمع البيانات الشخصية محدودًا ويتم بوسائل قانونية وعادلة. للأشخاص الخاضعين للبيانات الحق في إعطاء موافقتهم قبل معالجة بياناتهم. يجب أن تتم معالجة المعلومات الصحية المحمية بطريقة قانونية وعادلة وشفافة.

- **تحديد الغرض**
يجب أن يتم تحديد الغرض من جمع البيانات الشخصية قبل أو عند جمعها، وأي استخدام لاحق يجب أن يقتصر على تحقيق هذا الغرض. لا يجوز استخدام البيانات لغرض ثانوي إلا بموافقة صريحة من الشخص المعني أو بموجب القانون.

- **تقليل البيانات**
يجب أن تكون البيانات التي يتم جمعها كافية وذات صلة ولا تتجاوز ما هو ضروري للأغراض التي جُمعت من أجلها.

- **الدقة**
تلتزم شركة العربية بضمان دقة البيانات، واتخاذ خطوات معقولة لضمان تحديثها وتصحيحها فورًا عند اكتشاف أي خطأ.

- **ضمانات الأمان**
يجب حماية البيانات الشخصية من خلال ضمانات أمنية مناسبة لمنع التسرب أو الوصول غير المصرح به أو التعديل أو الحذف.

- **الأمان المادي والبيئي**
يجب أن يتم تأمين البيئة الفيزيائية (مثل غرف الخوادم والأرشيفات) والأنظمة المستخدمة لمعالجة وتخزين البيانات. ويجب اتخاذ إجراءات دورية لاختبار فعالية هذه التدابير.

- **الاحتفاظ / التخزين / الأرشفة / إعادة الاستخدام**
يجب حفظ أصول المعلومات الصحية داخل مراكز بيانات داخل الدولة ولمدة لا تقل عن 25 عامًا وفقًا لقانون الإمارات. ويجب التخلص منها بأمان عندما تنتهي فترة الحفظ مع توثيق كافة مراحل الإزالة.

- **مشاركة الأفراد**

للمستخدم الحق في معرفة ما إذا كانت هناك بيانات تخصه، ولأي غرض، ومن هي الجهات التي تتعامل مع هذه البيانات. وله الحق في الاعتراض على المعلومات أو تعديلها أو حذفها في حال ثبوت خطأ فيها.

VII. المعلومات الصحية المحمية(PHI)

VI.1 المعالجة

تشمل المعلومات الصحية المحمية (PHI) معلومات شخصية حساسة تتعلق بالأشخاص الخاضعين للبيانات، مثل الاسم الكامل، العنوان، أرقام الهواتف، البريد الإلكتروني، رقم الهوية، رقم السجل الطبي، أرقام الحسابات البنكية، صور الوجه، البيانات البيومترية، وعناوين IP. يجب أن تكون معالجة هذه المعلومات قانونية وآمنة وضمن الأطر التنظيمية لدولة الإمارات وقوانين الصحة في دبي.

VI.2 موافقة صاحب البيانات

يجب على الشركة إعلام أصحاب البيانات بكيفية استخدام معلوماتهم الصحية المحمية، والجهات التي يمكن أن تُفصح لها هذه المعلومات. تتطلب أي استخدام ثانوي للبيانات (مثل الأبحاث أو التسويق) موافقة صريحة وخطية من صاحب البيانات، ما لم يكن هناك استثناء قانوني محدد كما هو منصوص عليه في القوانين الإماراتية.

الحالات التي يمكن فيها معالجة البيانات بدون موافقة:

- البيانات الصحية :

1. المعلومات التي تطلبها شركات التأمين الصحي أو الاطراف الاخرى من مزودي الرعاية الصحية لاغراض التدقيق , الموافقة او التحقق من الاستحقاقات المالية المتعلقة بتلك الخدمات.
2. اغراض البحث العلمي شريطة عدم كشف هوية صاحب البيانات.
3. ان تكون المعالجة ضرورية لاتخاذ اجراءات وقائية و علاجية تتعلق بالصحة العامة.
4. بناء على طلب الجهة القضائيةاو طلب هيئة الصحة و لاغراض الرقابة و التفتيش.
5. ان تكون المعالجة ضرورية لممارسة صاحب البيانات حقوقه القانونية من اجراءات المطالبات و الدعاوى و الشكاوى.
6. ان تكون المعالجة ضرورية لاغراض قيام المتحكم (المنشأة) بالتزاماته و امتثاله للقوانين.
7. ان تكون المعالجة ضرورية لاغراض الطب الوقائي و لضمان معايير الجودة و و سلامة الرعاية الصحية و المنتجات الطبية.
8. لغرض تنفيذ عقد يكون صاحب البيانات طرف فيه.

- البيانات العامة:

يُحظر معالجة البيانات الشخصية دون موافقة صاحبها، وتُستثنى أي من الحالات التالية من هذا الحظر وتعتبر المعالجة حينها مشروعة:

1. أن تكون المعالجة ضرورية لحماية المصلحة العامة.
2. أن تكون المعالجة مرتبطة بالبيانات الشخصية التي أصبحت متاحة ومعلومة للكافة بفعل من صاحب البيانات.
3. أن تكون المعالجة ضرورية لإقامة أي من إجراءات المطالبة بالحقوق والدعاوى القانونية أو الدفاع عنها أو تتعلق بالإجراءات القضائية أو الأمنية.
4. أن تكون المعالجة ضرورية لأغراض الطب المهني أو الوقائي من أجل تقييم قدرة الموظفين على العمل، أو التشخيص الطبي أو تقديم الرعاية الصحية أو الاجتماعية أو العلاج أو خدمات التأمين الصحي أو إدارة أنظمة وخدمات الرعاية الصحية أو الاجتماعية وفقاً للتشريعات السارية في الدولة.
5. أن تكون المعالجة ضرورية لحماية الصحة العامة، وتشمل الحماية من الأمراض السارية والأوبئة أو لأغراض ضمان سلامة وجودة الرعاية الصحية والأدوية والعقاقير والأجهزة الطبية، وفقاً للتشريعات السارية في الدولة.
6. أن تكون المعالجة ضرورية لأغراض أرشيفية أو دراسات علمية وتاريخية وإحصائية وفقاً للتشريعات السارية في الدولة.
7. أن تكون المعالجة ضرورية لحماية مصالح صاحب البيانات.
8. أن تكون المعالجة ضرورية لأغراض قيام المتحكم أو صاحب البيانات بالتزاماته ومباشرة حقوقه المقررة قانوناً في مجال التوظيف أو الضمان الاجتماعي أو القوانين المعنية بالحماية الاجتماعية وذلك بالقدر الذي يسمح به في تلك القوانين.
9. أن تكون المعالجة ضرورية لتنفيذ عقد يكون صاحب البيانات طرفاً فيه أو لاتخاذ إجراءات بناءً على طلب صاحب البيانات بهدف إبرام عقد أو تعديله أو إنهائه.
10. أن تكون المعالجة ضرورية لتنفيذ التزامات محددة في قوانين أخرى في الدولة على المتحكم.

VI.3 أطراف ثالثة

في حال تعاقد الشركة مع جهة خارجية لمعالجة المعلومات، يجب التأكد من التزام هذه الجهة بالضوابط الأمنية والتنظيمية عبر اتفاقية مكتوبة. كما يجب استخدام تقنيات التشفير عند نقل البيانات، ويجب أن تشمل الاتفاقية بنودًا تتعلق بالسرية حتى بعد انتهاء العقد.

VI.4 النقل والتخلص

لا يجوز نقل المعلومات الصحية المحمية خارج الإمارات إلا إذا كانت ضمن الاستثناءات المنصوص عليها في قوانين الصحة. يجب أن يتم أي نقل أو مشاركة للبيانات بطريقة آمنة (مثل التشفير)، ويجب التخلص من البيانات بشكل نهائي وفق المعايير الوطنية.

VI.5 خرق حماية البيانات والسرية

يحدث خرق للبيانات عند الإتلاف أو الفقد أو التعديل أو الكشف أو الوصول غير المصرح به إلى المعلومات الصحية المحمية .(PHI) وتُعد هذه الحوادث خطيرة وقد تؤثر سلبًا على المرضى وسمعة الشركة.

أمثلة على حالات سوء السلوك:

- الكشف غير القانوني عن معلومات صحية محمية.
- الدخول إلى سجلات بدون سبب طبي واضح.

- إرسال معلومات حساسة إلى الشخص الخطأ.
- سرقة أجهزة تحتوي على.PHI
- إعادة تعريف بيانات تم إخفاء هويتها بدون إذن.

VI.6 الاستجابة للحوادث والتبليغ

يجب أن يكون لدى شركة العربية إجراء معتمد للاستجابة لحوادث الأمن المعلوماتي يشمل:

- تسجيل وتصنيف وترتيب أولوية الحوادث.
- تشخيص الحادث وتصعيده ومعالجته.
- التحقيق وجمع الأدلة، مثل لقطات الشاشة وسجلات الدخول.
- إخطار الجهات التنظيمية مثل هيئة الصحة بدبي ومكتب البيانات خلال الفترة المحددة.
- إخطار صاحب البيانات في حال كان هناك خطر كبير على خصوصيته.

VI.7 حماية البيانات حسب التصميم والإعداد الافتراضي

يجب أن يتم دمج حماية البيانات من المراحل الأولى لأي مشروع أو نظام جديد، بما يشمل التقييد بالغرض، تقليل البيانات، وإخفاء الهوية، من أجل حماية حقوق الأفراد طوال دورة حياة معالجة البيانات.

VI.8 حقوق صاحب البيانات على المعلومات الصحية المحمية

تلتزم شركة العربية بحماية حقوق الأفراد فيما يخص بياناتهم الصحية المحمية، حسب قانون حماية البيانات الاتحادي لدولة الإمارات. ومن هذه الحقوق:

- معرفة ما إذا كانت الشركة تحتفظ ببياناتهم والغرض من معالجتها.
- تلقي نسخة مفهومة من بياناتهم.
- تعديل أو حذف أو تصحيح البيانات الخاطئة.

VI.9 أنظمة تكنولوجيا المعلومات(IT)

يجب أن تضمن شركة العربية أن تكون أنظمة تكنولوجيا المعلومات محمية بوسائل تحكم مناسبة لمنع فقدان البيانات أو معالجتها بطريقة غير قانونية أو الوصول غير المصرح به إليها. ويجب أن يتضمن ذلك تطبيق معايير التحكم في الوصول على الأنظمة الصحية.

VI.10 إدارة الأجهزة (الطبية وغير الطبية)

يجب تسجيل وتتبع جميع الأجهزة من خلال قسم إدارة الأصول أو قسم الهندسة الطبية. ويجب توثيق تحركات الأجهزة وحذف البيانات الحساسة منها قبل التخلص منها أو إعادة استخدامها.

VI.11 إدارة وسائط التخزين القابلة للإزالة

يجب حفظ وسائط التخزين المتنقلة في بيئة آمنة. وينبغي مسح جميع البيانات منها قبل استخدامها من قبل أي شخص آخر. يجب تطبيق التشفير حيثما كان ذلك مطلوبًا، وتوثيق جميع الحركات الخاصة بالوسائط.

VI.12 الأمن الفيزيائي وضوابط الوصول إلىPHI/HIA

يجب تطوير سياسات وإجراءات لضبط استخدام والوصول إلى المعلومات الصحية بناءً على دور كل موظف أو طرف ثالث. ولا يجوز الوصول إلى سجلات المرضى إلا للأغراض المصرح بها. وأي استخدام أو مشاركة لكلمات المرور يعتبر خرقًا تأديبيًا.

VI.13 معالجة PHI من خلال منصة نبض(Nabidh HIE)

يجب الحصول على موافقة صريحة من المريض قبل الوصول إلى معلوماته الصحية عبر منصة نبض. كما يجب توفير خيار الانسحاب في أي وقت. وتظل الموافقة سارية المفعول حتى يقرر المريض الانسحاب منها.

VII. تصنيف أصول المعلومات الصحية(HIA)

تشمل الأصول المعلوماتية جميع أشكال البيانات وأنظمتها والبنية التحتية الداعمة. يجب تصنيف جميع الأصول حسب الحساسية والمخاطر وفقًا للفئات التالية:

- بيانات عامة / مفتوحة
- بيانات سرية
- بيانات حساسة
- بيانات سرية للغاية

VIII. إعادة تصنيف أصول المعلومات الصحية

يجب إعادة تقييم تصنيف الأصول عند الضرورة. ويمكن ترقية أو تخفيض التصنيف وفقًا للمخاطر المحتملة. وتقع مسؤولية هذا التغيير على مالك الأصل المعلوماتي.

IX. وضع ملصقات على الأصول الصحية

يجب وضع علامات واضحة على جميع الأصول الإلكترونية والفيزيائية لتحديد مستوى السرية. ويُفضل استخدام نص كبير وواضح بلون مميز (مثل الأحمر) مع تحديد التصنيف في أعلى وأسفل الصفحة.

X. تصاريح الوصول إلى أصول المعلومات الصحية داخل الشركة

لا يُسمح لأي فرد بالوصول إلى الأصول المصنفة على أنها سرية أو حساسة أو سرية للغاية بدون تصريح مسبق. يجب تطبيق مبدأ المعرفة اللازمة فقط، والمراجعة الدورية للتصاريح.

XI. إدارة أصول المعلومات الصحية

يجب اعتبار إدارة أصول المعلومات الصحية مسؤولية مؤسسية، ويجب معالجتها وتخزينها حسب تصنيفها.

XII. استخدام الحلول السحابية

يجب الامتثال للقوانين الإماراتية عند استخدام حلول تخزين سحابي. يجب أن تكون جميع البيانات داخل حدود الدولة، ويجب أن ينص العقد على استرداد البيانات وتدميرها عند انتهاء العلاقة مع المزود.

XIII. رقمنة السجلات الطبية

لتحسين الكفاءة، يجب على شركة العربية رقمنة السجلات الطبية الورقية إلى نسخ إلكترونية خلال مدة لا تتجاوز عامين من تاريخ إصدار هذا الميثاق. يجب تنفيذ رقابة جودة على الوثائق المرقمنة، والتأكد من مطابقتها للأصل قبل التخلص من النسخ الورقية بعد 60 يومًا.

XIV. استمرارية الأعمال / خطط التعافي من الكوارث

يجب على شركة العربية وضع سياسات وخطط موثقة لاستمرارية الأعمال واستعادة البيانات في حالات الكوارث. ويجب اختبار هذه الخطط بانتظام وتعيين موظفين مدربين لتنفيذها عند الحاجة.

XV. التدريب

يجب توفير برامج تدريب وتوعية لجميع الموظفين والموردين والمقاولين حول حماية البيانات. ويعد التدريب إلزاميًا عند التوظيف ويتكرر كل سنتين. كما يجب مراجعة محتوى البرامج التدريبية بشكل دوري لمواكبة القوانين واللوائح.

XVI. إغلاق أو اندماج الشركة

تستمر التزامات الشركة بتوفير البيانات للمرضى والجهات الصحية حتى بعد إغلاق أو اندماج الشركة، وفق ما تنص عليه سياسة إدارة أصول المعلومات الصحية الصادرة عن هيئة الصحة بدبي.

XVII. المساءلة

تتحمل شركة العربية المسؤولية الكاملة عن الامتثال للقوانين واللوائح ذات الصلة، ويجب أن تكون قادرة على إثبات هذا الامتثال. ويجب عليها تنفيذ تدقيقات دورية داخلية وخارجية، وتقديم نتائجها لهيئة الصحة بدبي سنويًا.

XVIII. المراقبة والامتثال

يجب على الشركة وضع خطة لرصد الامتثال لهذا الميثاق من خلال ضوابط مادية وفنية وإجرائية. وفي حال وجود انحرافات مبررة، يجب الحصول على موافقة هيئة الصحة بدبي. ويجب تقديم إعلان نضج من طرف ثالث ودمجه في التقرير السنوي.

XIX. عدم الامتثال

يُعد عدم الامتثال لهذا الميثاق انتهاكًا يتطلب التحقيق، وقد يؤدي إلى اتخاذ إجراءات تأديبية أو الفصل وفقًا للتشريعات السارية.

XX. الملحق - أ:

	التأثير المحتمل		
الهدف الأمني	منخفض	متوسط	عالِ
السرية: الحفاظ على القيود المصرح بها على الوصول إلى المعلومات والإفصاح عنها، بما في ذلك الوسائل المستخدمة لحماية الخصوصية الشخصية والمعلومات المملوكة.	قد يُتوقع أن يؤدي الكشف غير المصرح به عن المعلومات إلى تأثير ضار محدود على عمليات المنظمة أو أصولها أو الأفراد.	قد يُتوقع أن يؤدي الكشف غير المصرح به عن المعلومات إلى تأثير ضار خطير على عمليات المنظمة أو أصولها أو الأفراد.	قد يُتوقع أن يؤدي الكشف غير المصرح به عن المعلومات إلى تأثير ضار شديد أو كارثي على عمليات المنظمة أو أصولها أو الأفراد.
السلامة (النزاهة): الحماية من التعديل أو التدمير غير الصحيح للمعلومات، ويشمل ذلك ضمان عدم التنصل من المعلومات وأصالتها	قد يُتوقع أن يؤدي التعديل أو التدمير غير المصرح به للمعلومات إلى تأثير ضار محدود على عمليات المنظمة أو أصولها أو الأفراد.	قد يُتوقع أن يؤدي التعديل أو التدمير غير المصرح به للمعلومات إلى تأثير ضار خطير على عمليات المنظمة أو أصولها أو الأفراد.	قد يُتوقع أن يؤدي التعديل أو التدمير غير المصرح به للمعلومات إلى تأثير ضار شديد أو كارثي على عمليات المنظمة أو أصولها أو الأفراد.
التوافر: ضمان الوصول إلى المعلومات واستخدامها في الوقت المناسب وبشكل موثوق.	قد يُتوقع أن يؤدي تعطيل الوصول إلى المعلومات أو نظام المعلومات أو استخدامهما إلى تأثير ضار محدود على عمليات المنظمة أو أصولها أو الأفراد.	قد يُتوقع أن يؤدي تعطيل الوصول إلى المعلومات أو نظام المعلومات أو استخدامهما إلى تأثير ضار خطير على عمليات المنظمة أو أصولها أو الأفراد.	قد يُتوقع أن يؤدي تعطيل الوصول إلى المعلومات أو نظام المعلومات أو استخدامهما إلى تأثير ضار شديد أو كارثي على عمليات المنظمة أو أصولها أو الأفراد.

XXI. الملحق - ب

التصنيف	وصف الفئة	تأثير اختراق المعلومات	أمثلة
البيانات المفتوحة / العامة	معلومات معدة للاستخدام في المجال العام ولا توجد عليها قيود قانونية أو تنظيمية أو مؤسسية للوصول أو الاستخدام. - الغرض من إنشائها واستخدامها هو النفع العام، وتعزيز مصلحة المؤسسة أو الدولة، وتوفير معلومات جوهرية لتمكين المواطنين والمرضى وغيرهم من فهم رؤية وقيم الدولة أو الحكومة أو المؤسسة. - يُوصى بالتشفير. - يجب أن يتوافق استخدام وإصدار البيانات المفتوحة مع قوانين حقوق النشر المعمول بها.	لا يوجد تأثير	- المجالات العامة -نشرات معلومات المرضى - البيانات الصحفية والإعلانات - الإيداعات التنظيمية مثل تقارير ضريبة الدخل - علامات الاعتماد مثل اعتماد اللجنة المشتركة - المنشورات البحثية - منشورات التوعية العامة بالصحة أو الأنظمة - المواد العامة للبيع أو التسويق - معلومات الاتصال التجارية
سري	- معلومات يجب حمايتها بسرية محدودة نظرًا لاستخدامها في العمليات اليومية. - معلومات تتعلق بوظائف المؤسسة الداخلية ولا تهم جمهورًا أوسع. - حتى وإن لم تكن المعلومات الفردية حساسة، فقد تكشف في مجموعها معلومات أكثر مما يجب إذا تم الكشف عنها.	- قد يؤدي اختراق هذه المعلومات إلى انتهاك القانون الاتحادي لدولة الإمارات، أو القانون المحلي لإمارة دبي، أو سياسات ولوائح هيئة الصحة بدبي. - التسبب بضرر محدود للمصلحة العامة أو سمعة المؤسسة أو الأفراد. - ضرر محدود في الجوانب المالية. - التأثير سلبًا على قدرة المؤسسة التنافسية. -التأثير على السلامة العامة أو العدالة.	- العمليات والخدمات الروتينية - محاضر الاجتماعات، السياسات الداخلية، الإجراءات التشغيلية الموحدة، التعاميم الداخلية، العقود للمشاريع غير الحرجة، تقارير الأداء - المراسلات الداخلية أو مع جهات خارجية - التقارير والمعاملات المالية - وثائق اتخاذ القرار السرية - الأنظمة والسياسات والمعايير والإجراءات الداخلية
حساس	- معلومات تتطلب حماية قوية نظرًا لدورها الحاسم في صنع القرار داخل المؤسسة أو عبر القطاع الصحي والحكومة. - معلومات قد تكشف تصاميم أو تكوينات أو ثغرات يمكن استغلالها من قبل جهات خبيثة. - معلومات تلتزم المؤسسة أو الحكومة بحمايتها بموجب التفويض التنظيمي.	- قد يؤدي اختراق هذه المعلومات إلى انتهاك القانون الاتحادي لدولة الإمارات، أو القانون المحلي لإمارة دبي، أو سياسات ولوائح هيئة الصحة بدبي. - تعطيل أو فقدان قدرات الطوارئ والرعاية الصحية، فقدان ثقة الجمهور في القطاع الصحي، أو ضرر كبير لسمعة القطاع الصحي مع تغطية إعلامية واسعة. - التأثير سلبًا على القدرة التنافسية للمؤسسة. - التأثير على السلامة العامة أو العدالة.	- السجلات الطبية والمعلومات الصحية الشخصية - معلومات طبية حساسة: * الإدمان * فيروس نقص المناعة البشرية * الأمراض النفسية * الصحة السلوكية * ملاحظات العلاج النفسي * إساءة استخدام المواد الكحولية * الصحة الإنجابية * المعلومات الجينية * الصحة الجنسية (بما في ذلك الأمراض المنقولة جنسيًا) * بيانات حمل الأطفال * حالات إساءة معاملة الأطفال - عقود أو طلبات مشاريع استراتيجية/حرجة - تقارير التدقيق - سجلات المخاطر والأصول - التفاصيل المالية المتعلقة بالمشاريع أو العروض - تقارير حوادث أمن المعلومات - ملفات الموارد البشرية / معلومات شخصية عن الموظفين - السجلات التعليمية التعريفية الشخصية - معلومات سرية عن إدارة المؤسسة - سجلات المحاكم - سجلات التبني

			- سجلات التحقيقات، الشكاوى، والانتهاكات - اتفاقيات أو عقود ذات طبيعة سرية بين المؤسسة وجهات داخل الإمارات أو دوليًا
سري للغاية	- معلومات تتطلب حماية متعددة المستويات نظرًا لطبيعتها شديدة الحساسية.	- الكشف عن هذه المعلومات للعامة أو تبادلها داخل الحكومة بشكل غير مصرح به يعتبر غير قانوني وقد يتسبب بأضرار جسيمة للأفراد، الحكومة، الأمن الوطني، التماسك الاجتماعي، الاستقرار الاقتصادي وصحة الدولة. - قد يهدد الحياة، أو يؤثر بشكل خطير على النظام العام، ويسبب تمييزًا، أو سوء معاملة، أو إهانة، أو تقويض كرامة أو سلامة الأشخاص.	- السجل الطبي لشخصيات هامة (VIP) - بيانات قوى الأمن - قارير أو أوامر أمنية أو محاضرها - تقارير ومحاضر حساسة للمجلس التنفيذي ولجانه - اتفاقيات أو عقود بين إمارة دبي وأخرى، أو بين دولة الإمارات ودول أخرى - بيانات شهود في قضايا خطيرة -تفاصيل بطاقات الائتمان / معلومات الدفع - معلومات فنية خاضعة للرقابة ("CTI") - عناوينIP - مخططات الشبكات والبنية التحتية

XXII. الملحق – ج

متطلبات التحكم في الوصول لأصول المعلومات الصحية	
التصنيف	**متطلبات التحكم في الوصول**
البيانات المفتوحة / العامة	- متاحة للجمهور. - يمكن مشاركتها مع أطراف ثالثة دون الحاجة إلى إذن.
سري	- متاحة للمستخدمين المصرح لهم فقط. - تتم المشاركة بموافقة مالك أصل المعلومات الصحية.
حساس	- متاحة فقط للمستخدمين المصرح لهم. - يجب على مالكي أصول المعلومات تطبيق ضوابط وصول أكثر صرامة. - يمكن مشاركتها مع الجهات الحكومية / الخاصة: * بموافقة الفرد المعني. * حسب ما يتطلبه العقد، مع مراعاة قيود عدم الإفصاح واتفاقية مشاركة البيانات المناسبة. * بناءً على إعفاء من التفويض صادر عن مجلس مراجعة مؤسسي مخول. - يجب تسجيل الوصول إلى هذه المعلومات ومراجعته من قبل مالك أصل المعلومات.
سري للغاية	- يمكن الوصول إلى هذه المعلومات فقط: * إذا كان ذلك مطلوبًا بموجب القانون أو اللوائح. * بناءً على أمر صادر بشكل قانوني. * إذا لزم الأمر خلال إجراء قانوني.

XXIII. الملحق - د

الفئة	بيانات مفتوحة/ عامة	سري	حساس	سري للغاية
المواد المطبوعة	لا توجد متطلبات خاصة. يُفضل إعادة التدوير.	-يُخزّن في مكان آمن. -الحفاظ على مكتب نظيف؛ يجب على أعضاء الفريق "تفريغ مكاتبهم" في نهاية كل يوم عمل. -يجب تصنيف الوثائق حسب فئتها (سري/حساس/سري للغاية). -يجب تطبيق تدابير الأمان الفيزيائي والبيئي (مثل النسخ الاحتياطي، التخزين في خزائن مقاومة للحريق، إلخ) لضمان المعالجة والتخزين والمشاركة والاستضافة والتخلص الآمن من المعلومات الصحية. -يجب التخلص منها في حاوية مخصصة ومعلمة بوضوح للتمزيق أو الإتلاف (إلا في حال كانت خاضعة لإيقاف قانوني).	(نفس متطلبات "سري")	(نفس متطلبات "سري")
الوثائق الإلكترونية	لا توجد متطلبات خاصة	-يجب التخزين على أجهزة معتمدة من الجهة. -التحكم في الوصول وإمكانية الطباعة. -التخزين فقط على محركات الشبكة الآمنة (وليس على الأقراص الصلبة أو سطح المكتب). -يجب تصنيف الوثائق المملوكة أو المُنشأة من قبل الجهة حسب فئتها (سري/حساس/سري للغاية).	(نفس متطلبات "سري")	(نفس متطلبات "سري")
الأجهزة والمعدات الطبية	لا توجد متطلبات خاصة	-يتطلب اهتمامًا خاصًا بالتحكم في الوصول، والمصادقة، والتفويض، وإجراءات التعامل، وسجل المخاطر، والتخلص الآمن من المعدات والأجهزة الطبية.	(نفس متطلبات "سري")	(نفس متطلبات "سري")
الوسائط الإلكترونية) مثلUSB ، الأقراص الصلبة، الأقراص المضغوطة(	لا توجد متطلبات خاصة	-يجب التخزين على أجهزة معتمدة من الجهة. -التحكم في الوصول وإمكانية الطباعة. -التخزين في مكان آمن. -استخدام التشفير المعتمد من الجهة. -لا يجوز إعادة استخدام الوسائط الخاضعة لإيقاف قانوني. -في حال إعادة استخدام وسائط أخرى، يجب إزالة جميع البيانات أولًا من قبل قسم خدمات المعلومات. -يجب التخلص من الوسائط الإلكترونية بطريقة آمنة. -يجب إتلاف جميع الوسائط المستغنى عنها وفقًا لمتطلبات معيار ISO 27001:2013 ومعايير	- يجب تأمين وسائط النسخ الاحتياطي ماديًا. - يجب أن تكون وسائط النسخ الاحتياطي المخزنة خارج الموقع مشفرة. - يجب جعل وسائط النسخ الاحتياطي غير قابلة للقراءة قبل التخلص منها.	(نفس متطلبات "حساس")

		تنظيم أمن المعلومات (ISR) الصادرة عن حكومة دبي الذكية.		
الأجهزة المحمولة	لا توجد متطلبات خاصة	-يجب تكوين الأجهزة المحمولة لمنع الاستخدام غير المصرح به. -يجب أن تستخدم جميع الأجهزة المحمولة التشفير. -يجب تشفير الاتصالات بين الأجهزة المحمولة المصرح بها وسجلات المرضى الإلكترونية. -يجب تخزين الأجهزة المحمولة في مكان آمن.	(نفس متطلبات "سري")	(نفس متطلبات "سري")
البريد الإلكتروني	لا توجد متطلبات خاصة	-لا يجوز مشاركة البيانات السرية عبر البريد الإلكتروني. -بالنسبة للبيانات الحساسة: •يجب استخدام نظام البريد الإلكتروني الخاص بالشركة. •يُسمح بإرسال الحد الأدنى من المعلومات الصحية الشخصية الضرورية فقط. •تأكد من عدم وجود معلومات صحية شخصية في عنوان الموضوع. •يجب إرسال المعلومات الصحية الشخصية كـ: o مرفق مؤمّن ومغلق) مثل PDF محمي بكلمة مرور (أو كرابط إلى بوابة المعلومات الصحية. •يجب استخدام إيصالات القراءة/الاستلام/التسليم إن أمكن. •إضافة إخلاء مسؤولية إلى توقيع البريد الإلكتروني يشير إلى أن الرسالة سرية وموجهة فقط للمستلم المقصود، مع إرشاد أي شخص يتلقى الرسالة عن طريق الخطأ إلى حذفها أو تمزيقها وإبلاغ المرسل. •يجب الاحتفاظ بنسخ من البريد الإلكتروني والمرفقات في ملف العميل، ويجب أن تكون معلومات التاريخ والوقت والمستلم واضحة.	(نفس متطلبات "سري")	(نفس متطلبات "سري")

XXIV. الملحق - هـ

الفئة	بيانات مفتوحة / عامة	حساس	سري للغاية
المواد المطبوعة	لا تتطلب معالجة خاصة. ينصح بإعادة التدوير	يجب التخلص منها في حاوية مخصصة بوضوح للفرم أو الإتلاف (ما لم تكن خاضعة لإيقاف قانوني).	يجب التخلص منها في حاوية مخصصة بوضوح للفرم أو الإتلاف (ما لم تكن خاضعة لإيقاف قانوني).
الوسائط الإلكترونية) مثل USB، الأقراص الصلبة، الأقراص المضغوطة(	لا تتطلب معالجة خاصة.	-الوسائط الخاضعة لإيقاف قانوني لا يجوز إعادة استخدامها. إذا تم إعادة استخدام وسائط أخرى، يجب إزالة جميع البيانات أولاً من قبل خدمات المعلومات - .يجب التخلص من الوسائط الإلكترونية بطريقة آمنة - .يجب تدمير جميع الوسائط المتروكة وفقًا لمتطلبات ISO 27001:2013ومعايير لائحة أمن المعلومات (ISR)الصادرة عن حكومة دبي الذكية.	-الوسائط الخاضعة لإيقاف قانوني لا يجوز إعادة استخدامها. إذا تم إعادة استخدام وسائط أخرى، يجب إزالة جميع البيانات أولاً من قبل خدمات المعلومات - . يجب التخلص من الوسائط الإلكترونية بطريقة آمنة - . يجب تدمير جميع الوسائط المتروكة وفقًا لمتطلبات ISO 27001:2013ومعايير لائحة أمن المعلومات (ISR)الصادرة عن حكومة دبي الذكية.