

**اختبار الأجسام المضادة المحايدة للفيروس المرتبط بالفيروس الغدي من النوع 5 (AAV5)
إشعار الخصوصية للمرضى والأطباء الذين يطلبون إجراء الاختبار**

1. تقوم شركة Precision for Medicine, Inc، الكائنة في 8440 Broadband Drive, Frederick, MD 21701، الولايات المتحدة الأمريكية (يُشار إليها باسم "Precision" أو الضمير "نحن") بجمع ومعالجة البيانات الشخصية الخاصة بما يلي:
أ. المرضى الذين خضعوا لاختبار الأجسام المضادة المحايدة للفيروس المرتبط بالفيروس الغدي من النوع 5 (AAV5) ("الاختبار")
ب. الأطباء الذين يطلبون إجراء الاختبار.

يُشار إلى المرضى والأطباء المعالجين مجتمعين في هذا الإشعار بضمير المخاطب "أنت"/"كاف الخطاب".

2. تلتزم شركة Precision بالشفافية بشأن كيفية جمع البيانات الشخصية ومعالجتها والوفاء بالتزامات حماية البيانات بموجب القوانين واللوائح المعمول بها.

3. في إشعار الخصوصية هذا، سنشرح البيانات الشخصية الخاصة بك التي يتم جمعها لغرض الاختبار، ومكان وكيفية معالجتها، ومدة الاحتفاظ بها، وكيف يمكنك ممارسة حقوقك المتعلقة بمعالجة البيانات. لفهم كيفية معالجة شركة Precision البيانات الشخصية على نطاق أوسع، يُرجى الرجوع إلى سياسة الخصوصية العالمية لدينا، والتي يمكن العثور عليها هنا:

<https://www.precisionmedicinelab.com/privacy/>

4. المتحكم في بياناتك الشخصية هو

شركة Precision for Medicine, Inc، الكائنة في 8440 Broadband Drive, Frederick, MD 21701، الولايات المتحدة الأمريكية.

5. إذا كانت لديك أي أسئلة حول إشعار الخصوصية هذا أو حول كيفية معالجتنا لبياناتك الشخصية، فيُرجى الاتصال بمسؤول حماية البيانات: privacy@precisionmedicinegrp.com

6. الغرض من معالجة البيانات:

أ. الغرض من معالجة بياناتك الشخصية هو إجراء الاختبار. بياناتك الشخصية مطلوبة من أجل:

1. طلب إجراء الاختبار بواسطة شركة Precision

2. تمكين Precision من استلام عينة الاختبار

3. تمكين Precision من إجراء الاختبار وتسجيل نتائج الاختبار

4. تمكين Precision من إعادة نتائج الاختبار

بالنسبة للطبيب المعالج، من خلال طلب إجراء اختبار، فإن هذا يعني أنك قد قرأت وفهمت محتويات إشعار الخصوصية هذا وتوافق على معالجة البيانات الشخصية على النحو المبين في إشعار الخصوصية هذا.

بالنسبة للمرضى، يجب الحصول على موافقتك من قبل طبيبك المعالج الذي يشارك بياناتك الشخصية مع شركة Precision كجزء من عملية العلاج الصحي ودائرة الرعاية. موافقتك هي الأساس القانوني الذي نعتمد عليه لمعالجة بياناتك الشخصية فيما يتعلق بتقديم الاختبار. إلا أنه في بعض الحالات، قد نكون ملزمين بالاحتفاظ ببياناتك الشخصية أو إجراء المزيد من المعالجة لبياناتك وفقاً لمتطلبات قانونية.

7. ما البيانات الشخصية التي نقوم بجمعها ومعالجتها؟

أ. نجمع البيانات الشخصية التالية الخاصة بالمرضى فيما يتعلق بالاختبار:

1. الاسم الأول والأوسط والأخير

2. تاريخ الميلاد

3. الجنس عند الولادة

4. رقم السجل الطبي

5. عينة الاختبار التي تم جمعها من المرضى بواسطة الطبيب مقدم طلب الاختبار

6. نتائج الاختبار (والتي ستتضمن بياناتك الحساسة (وتحديداً، بياناتك الصحية)).

كما ذكر أعلاه، يجب على الطبيب المعالج الحصول على موافقة المريض للإفصاح عن البيانات الشخصية المذكورة أعلاه إلى شركة Precision.

ب. نجمع البيانات الشخصية التالية للأطباء المعالجين فيما يتعلق بالاختبار:

1. الاسم الأول والأوسط والأخير
2. تفاصيل الاتصال (الهاتف، الفاكس، البريد الإلكتروني)
3. اسم مركز/منشأة الرعاية الصحية وعنوانها ومعلومات الاتصال بها

8. إلى متى سيتم الاحتفاظ ببياناتك الشخصية؟

أ. سنحتفظ ببياناتك الشخصية المرتبطة بالاختبار حسب الحاجة لإجراء الاختبار بشكل صحيح، والتحقق من نتائج الاختبار وإبلاغ الطبيب المعالج بنتائج الاختبار.

ب. سيتم الاحتفاظ ببياناتك الشخصية لمدة سبع (7) سنوات بعد الإبلاغ عن نتيجة الاختبار لضمان إمكانية فحص الجودة، وإعادة الاختبار، إذا لزم الأمر، وضمان حصول الطبيب المعالج على نتائج الاختبار.

ج. في نهاية فترة الاحتفاظ هذه، سيتم حذف بياناتك الشخصية.

9. حقوقك

أ. لديك حقوق فيما يتعلق ببياناتك الشخصية التي سنحتفظ بها لهذه الأغراض، والتي تتضمن ما يلي:

1. حق الوصول إلى بياناتك الشخصية – يحق لك الحصول على نسخة من بياناتك الشخصية، مع مراعاة بعض الاستثناءات والاعتبارات الأخرى التي يجب أن نأخذها في الحسبان عند تقييم طلبك.
2. حق تصحيح بياناتك الشخصية إذا كانت غير دقيقة – يحق لك طلب تصحيح أي أخطاء أو عدم دقة في بياناتك الشخصية. وكجزء من هذا الحق، يمكنك تقييد معالجة البيانات الشخصية التي تكون دقتها محل نزاع (حتى يتم التحقق منها).
3. حق حذف بياناتك الشخصية – يحق لك أن تطلب منا حذف بياناتك الشخصية في حالات معينة، وبشرط ألا يكون لدينا مبررًا أساسيًا للاحتفاظ بها.
4. حق سحب موافقتك – كما ذكرنا أعلاه، فإن الأساس القانوني لمعالجة بياناتك الشخصية في معظم الحالات هو الموافقة. إذا كنت ترغب في سحب موافقتك، فيمكنك القيام بذلك في أي وقت. لن يؤثر سحب الموافقة على شرعية استخدامنا لبياناتك الشخصية قبل سحب هذه الموافقة. إذا كنت ترغب في سحب موافقتك، فيرجى إرسال بريد إلكتروني إلى مسؤول حماية البيانات (DPO) لدينا على عنوان البريد الإلكتروني الوارد أدناه.

يُرجى العلم أنه قد لا تتمكن شركة Precision دائمًا من الالتزام الكامل بطلبك، حيث قد تفرض قوانين خدمات الرعاية الصحية والتشخيص الطبي على شركة Precision و/أو الطبيب المعالج الاحتفاظ بالبيانات الشخصية للمريض المتعلقة بإجراء الاختبار.

إذا كنت ترغب في ممارسة حقوقك، فيرجى إرسال رسالة إلكترونية إلى مسؤول حماية البيانات المعين على privacy@precisionmedicinegrp.com

10. مستلمو البيانات

ستشارك شركة Precision بياناتك الشخصية المستلمة مع الأطراف الضرورية بما في ذلك المعالجين المعيّنين بموجب عقد ملزم قانونًا لتقديم الخدمات إلى شركة Precision والتي تكون ضرورية لإجراء الاختبار بواسطة شركة Precision والحفاظ على البنية التحتية المختبرية المناسبة.

11. كيفية تقديم شكوى

إذا كانت لديك أي مخاوف بشأن بياناتك الشخصية التي تحتفظ بها شركة Precision، فيمكنك تقديم شكوى إلى الممثل التالي: privacy@precisionmedicinegrp.com

يحق لك أيضًا تقديم شكوى إلى هيئة حماية البيانات في المملكة العربية السعودية (الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)).

12. نقل بياناتك الشخصية خارج المملكة العربية السعودية

للسماح لشركة Precision بإجراء الاختبار بشكل صحيح، يتعين علينا نقل بياناتك الشخصية إلى دول خارج المملكة العربية السعودية، وتحديداً الولايات المتحدة الأمريكية. في مثل هذه الحالات، سنلتزم بقوانين حماية البيانات المعمول بها واتخاذ الإجراءات التي تفرضها القوانين لضمان خصوصية بياناتك الشخصية.

- بموجب قوانين حماية البيانات في المملكة، لا يُسمح بنقل بياناتك الشخصية إلى دولة أخرى إلا في الحالات التالية:
- إذا قررت الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) أو الجهة التنظيمية المختصة أن الدولة المستلمة للبيانات تضمن مستوى كافٍ من حماية البيانات الشخصية (أي أنها دولة ذات مستوى حماية كافٍ)؛
- إذا كانت هناك ضمانات مناسبة قائمة، إلى جانب حقوق قابلة للتنفيذ وسبل قانونية فعالة متاحة لك؛ أو
- إذا كان هناك استثناء محدد ينطبق بموجب قانون حماية البيانات في المملكة.

عندما ننقل بياناتك الشخصية خارج المملكة من أجل إجراء الاختبار، يخضع هذا النقل للبند التعاقدية القياسية التي تنشرها سدايا. في كل مرة يتم فيها نقل بياناتك الشخصية إلى شركة Precision لأغراض الاختبار، تُبرم شركة Precision هذه البنود التعاقدية القياسية مع الطرف الذي يرسل بياناتك الشخصية إلى شركة Precision لإضفاء الشرعية على هذا النقل ولتوفير حماية إضافية لبياناتك الشخصية. يكون الطبيب المعالج هو "مصدر البيانات الشخصية" وتكون شركة Precision هي "مستورد البيانات الشخصية".

يمكن العثور على نموذج البنود التعاقدية القياسية التي نستخدمها على الموقع الإلكتروني لسدايا <https://sdaia.gov.sa/Documents/StandardContractualClausesForPersonalDataTransferEN.pdf> يتم استكمال هذه البنود التعاقدية القياسية على النحو التالي

- يكون نموذج البنود التعاقدية القياسية المعمول بها هو النموذج الأول: المتحكم إلى المتحكم
- بالنسبة للملحق 1 – يكون الطبيب المعالج هو "مصدر البيانات الشخصية" وتكون شركة Precision هي "مستورد البيانات الشخصية".
- بالنسبة للملحق 2 - يجب أن تكون فئات البيانات الشخصية المنقولة والغرض من فترة النقل والاحتفاظ على النحو المحدد في نقاط إشعار الخصوصية 6 و 7 و 8 أعلاه
- بالنسبة للملحق 3 - يجب أن تكون التدابير الأمنية المطبقة على النقل على النحو التالي:

- يتعين على جميع موظفي شركة Precision إكمال تدريب الخصوصية ذي الصلة والمتخصص ويجب عليهم اجتياز تقييم قبل الوصول إلى البيانات الشخصية والبيانات ذات الفئة الخاصة.
- لدى Precision إجراءات تشغيل معيارية مطبقة، بما في ذلك إجراءات التعيين وإنهاء الخدمة، لضمان وصول الأفراد المصرح لهم فقط إلى البيانات الشخصية والبيانات ذات الفئة الخاصة. تتضمن إجراءات التشغيل المعيارية معلومات حول كيفية تعامل شركة Precision مع أنشطة المعالجة.
- هناك لجنة حوكمة لمراقبة أنشطة المعالجة والمخاطر المعلوماتية المرتبطة بها.
- لدى شركة Precision عدد من إجراءات التشغيل المعيارية (SOPs) المعنية بحوكمة أمن تكنولوجيا المعلومات، والمعلومات الاستخباراتية المتعلقة بالتهديدات السيبرانية، وأمن التطبيقات، وإدارة المخاطر.
- لدى شركة Precision إجراءات تشغيل معيارية وحلول معتمدة لإدارة التصعيد، والبحث الجنائي الرقمي للبيانات، والإبلاغ عن حوادث الأمان، والمراقبة المستمرة ضد التهديدات والثغرات الأمنية.
- يتم نقل البيانات من خلال بروتوكول أمان طبقة النقل (TLS) وبروتوكول نقل الملفات الآمن (SFTP)، ويتم تخزينها في حالة السكون باستخدام معايير التشفير المعتمدة في الصناعة (AES 256 على الأقل)، وسيتم تحديث ضوابط التشفير لتعكس التغييرات في معايير الصناعة. تستخدم Precision Medicine Group جدران الحماية مع أنظمة كشف ومنع التسلل. يتم تشفير جميع نقاط النهاية بقوة تشفير AES 256. يتضمن إطار عمل الأمان السيبراني لدى Precision الحلول التالية:

- اكتشاف نقطة النهاية والاستجابة لها (EDR)

- الاكتشاف المُدار والاستجابة المُدارة (MDR)

- مزود خدمات الأمان المُدارة (MSSP)

- وكيل الويب المعتمد على السمعة

- إدارة معلومات وأحداث الأمان (SIEM)

- فحص الشبكات الداخلية والخارجية

- تقييمات المخاطر المستمرة

- اختبار اختراق الشبكات والتطبيقات

- تطبق شركة Precision المصادقة متعددة العوامل للحد من مخاطر الوصول غير المصرح به وتطبق إجراءات تشغيل معيارية لضمان وصول الأفراد المعتمدين والمصرح لهم فقط إلى الأنظمة التي تعالج البيانات الشخصية.

- لدى شركة Precision خطة لاستمرارية الأعمال والتعافي من الكوارث والنسخ الاحتياطي والاستعادة لضمان القدرة على استعادة التوافر والوصول إلى البيانات الشخصية في الوقت المناسب في حالة وقوع حادث مادي أو فني.
- تُجري شركة Precision اختبارات وعمليات تدقيق منتظمة على بنيتها التحتية التقنية لتكنولوجيا المعلومات. كما يتم إجراء مراجعات التدقيق بشأن الوصول والاحتفاظ بها لتحديد الأفراد الذين لديهم حق الوصول إلى البيانات الشخصية وبيانات الفئات الخاصة.
- يستند إطار الأمن السيبراني لدى Precision إلى معايير NIST.
- لدى شركة Precision إجراء تشغيل معياري رسمي لتأهيل موردي تكنولوجيا المعلومات يضمن امتثال الموردين للضوابط التالية:
 - الامتثال لإطار الأمن السيبراني الخاص بشركة Precision
 - إجراء عمليات تدقيق سنوية متوافقة مع SOC 2 Type 2 للموردين المناسبين
 - الحصول على اعتماد ISO 27001 للموردين المناسبين
 - الامتثال لجميع إجراءات التشغيل المعيارية ذات الصلة الخاصة بتكنولوجيا المعلومات الدقيقة ومعالجة البيانات والخصوصية
- يجب أن تتضمن جميع عقود موردي Precision والمعالجين الفرعيين شروطاً وبنوداً متوافقة مع المادة 28