سياسة خصوصية البيانات

الجمعية السعودية لعلاج جذور وأعصاب الأسنان

المقدمة

تلتزم الجمعية السعودية لعلاج جذور وأعصاب الأسنان بحماية خصوصية وسرية بيانات جميع الأطراف المتعاملين معها، بما يتماشى مع:

- **نظام حماية البيانات الشخصية السعودي**.
- **المعايير الدولية لأمن المعلومات الصحية.**
- **قيم الجمعية في الشفافية والمساءلة**.

الأهداف:

تهدف هذه السياسة إلى تنظيم جمع ومعالجة البيانات لضمان:

✓حماية معلومات المرضى والباحثين والمتبرعين.

✓الامتثال للأنظمة المحلية والدولية.

✓تعزيز الثقة في خدمات الجمعية.

نطاق السياسة

تشمل هذه السياسة:

- **البيانات المجمعة عبر**:
  - الموقع الإلكتروني والتطبيقات الرقمية للجمعية.
  - الفعاليات (المؤتمرات، ورش العمل، الحملات التوعوية).
  - الأبحاث والدراسات العلمية.
- **الجهات الخاضعة**:
  - الموظفون والمتطوعون.
  - الشركاء والموردون.
  - أي طرف ثالث يتعامل مع بيانات الجمعية.

أنواع البيانات المجمعة

نوع البيانات	مستوى الحساسية	فترة الاحتفاظ
البيانات الشخصية (الاسم، الهوية، الاتصال)	عالي	5سنوات بعد آخر تفاعل
السجلات الطبية	عالي جدًا	15سنة
بيانات الأبحاث	متوسطة	10سنوات بعد نشر الدراسة
بيانات المتبرعين	متوسطة	7سنوات (وفق المتطلبات الضريبية)
بيانات الخدمة ((استشارات، حضور فعاليات)	منخفضة	3سنوات

أهداف معالجة البيانات

١. تقديم الرعاية الطبية والتوعوية لمستفيدي الجمعية.
٢. تطوير الأبحاث المتعلقة بأمراض جذور وأعصاب الأسنان.
٣. تحسين جودة الخدمات (المؤتمرات، الاستشارات).
٤. الوفاء بالمتطلبات القانونية والتنظيمية.

حقوق أصحاب البيانات

- **الحق في المعرفة** :الاطلاع على البيانات المحفوظة وأسباب جمعها.
- **الحق في التصحيح** :طلب تعديل البيانات غير الدقيقة.
- **الحق في الحذف** :طلب إزالة البيانات عند انتهاء الغرض منها.
- **الحق في الاعتراض** :رفض استخدام البيانات لأغراض تسويقية.

مشاركة البيانات مع أطراف ثالثة

الحالات المسموح بها	الحالات الممنوعة
بموافقة صريحة من صاحب البيانات.	**مشاركة البيانات لأغراض تجارية غير مصرح بها.**
عند وجود أمر قضائي أو طلب رسمي من الجهات المختصة.	**مع جهات غير خاضعة لمعايير حماية مماثلة.**
مع الشركاء الطبيين المعتمدين (مثل المستشفيات الجامعية).	

إجراءات حماية البيانات

الحماية التقنية:

- تشفير البيانات المخزنة والمتنقلة
- نسخ احتياطي دوري في مواقع آمنة.
- استخدام جدران حماية وأنظمة كشف الاختراقات.

الحماية الإدارية:

- اتفاقيات مع جميع العاملين
- تقييد الوصول حسب مبدأ "أقل صلاحية"
- تدريب سنوي على أمن المعلومات للموظفين

حماية البيانات البحثية:

- إزالة المعلومات التعريفية (مثل الأسماء، الهويات) قبل تحليل البيانات.
- تخزين البيانات المجهولة في أنظمة منفصلة.

إجراءات الاستجابة للانتهاكات

١. **الكشف:**
   - رصد أي خرق خلال **24ساعة** عبر أنظمة المراقبة

٢. **الاحتواء:**
   - عزل الأنظمة المتأثرة فورًا.

٣. **الإبلاغ:**
   - إخطار الجهات التنظيمية خلال ٧٢ ساعة
   - إعلام الأفراد المعنيين إذا كانت البيانات المكشوفة حساسة.

٤. **التقييم:**
   - تحليل جذور المشكلة وإصلاح الثغرات.

٥. **المنع:**
   - تحديث الضوابط الأمنية لمنع التكرار.

تحديثات السياسة

- تُراجع السياسة **سنويًا** أو عند وجود تغييرات تشريعية.
- يتم إعلام المستفيدين بالتحديثات عبر:
  - البريد الإلكتروني.
  - إشعار في الموقع الإلكتروني.
  - رسائل SMS للحالات الحرجة.