حماية البيانات الصحية للمرضى في ظل تطبيقات الصحة الرقمية

Protection of Patient Health Data in the Context of Digital Health Applications

محمد عبود حامد محمد*، قسم الحقوق، كلية العلوم الإدارية والإنسانية، كليات بريدة الأهلية –المملكة العربية السعودية–
wedabboud@gmail.com
شذى حامد عمر محمد، كلية الشريعة والقانون، جامعة الزعيم الأزهري –السودان–
shazaomar59@gmail.com

تاريخ إرسال المقال: 2025/07/11 تاريخ قبول المقال: 2025/10/29 تاريخ نشر المقال: 2025/11/29

الملخص:

تتناول هذه الورقة البحثية التحديات المتزايدة لحماية بيانات المرضى في عصر الصحة الرقمية. تحلل الورقة طبيعة البيانات الصحية الرقمية والمخاطر السيبرانية والأخلاقية المحدقة بها، خاصة تلك الناشئة عن استخدام الذكاء الاصطناعي .كما تستعرض الأطر القانونية الدولية (GDPR, HIPAA) والإقليمية (PDPL) والضمانات التقنية المتاحة. وتخلص إلى أن الحماية الفعالة تتطلب نهجاً شمولياً يدمج بين التشريع الصارم، والحوكمة الأخلاقية، والضوابط التقنية الاستباقية، لضمان الثقة في المنظومة الصحية الرقمية.

الكلمات المفتاحية: حماية البيانات، الصحة الرقمية، خصوصية المريض، السجلات الصحية الإلكترونية، تطبيقات الصحة المتنقلة.

Abstract:

This research paper addresses the growing challenges of protecting patient data in the digital health era. The paper analyzes the nature of digital health data and the associated cyber and ethical risks, particularly those arising from the use of Artificial Intelligence. It also reviews international (GDPR, HIPAA) and regional (PDPL) legal frameworks and available technical safeguards. It concludes that effective protection requires a comprehensive approach integrating robust legislation, ethical governance, and proactive technical controls to ensure trust in the digital health ecosystem.

Key words: Data Protection, Digital Health, Patient Privacy, Electronic Health Records, mHealth.

مقدمة:

يشهد العالم مفارقة محورية في عصر الصحة الرقمية؛ ففي الوقت الذي تُحدث فيه التقنيات الرقمية ثورة في نماذج تقديم الرعاية الصحية، وتعزز من قدرات التشخيص والعلاج وتفتح آفاقاً للطب الشخصي والوقائي، فإنها في المقابل تخلق تحديات غير مسبوقة لخصوصية المريض وأمن بياناته. إن البيانات الصحية، بطبيعتها،

* المؤلف المرسل

تعد من أكثر أنواع البيانات الشخصية حساسية، حيث يكشف المساس بها عن أدق تفاصيل حياة الفرد الصحية والجسدية، وقد يعرضه لمخاطر التمييز والوصم الاجتماعي.

تتمحور إشكالية هذا البحث حول الفجوة المتنامية بين سرعة الابتكار التكنولوجي في جمع ومعالجة البيانات الصحية وتنوع مصادرها، وبين بطء تطور الأطر القانونية والأخلاقية والتقنية اللازمة لتوفير حماية كافية ومواكبة لهذه التطورات (1). فمن السجلات الصحية الإلكترونية الشاملة، إلى تطبيقات الصحة المتنقلة التي لا حصر لها، والأجهزة القابلة للارتداء التي تراقب مؤشراتنا الحيوية على مدار الساعة، أصبحت بياناتنا الصحية تُجمع وتُخزن وتُشارك وتُحلل على نطاق لم يسبق له مثيل، وغالباً في بيئات تفتقر إلى الضوابط الأمنية الكافية أو الشفافية اللازمة.

تنبع أهمية هذا البحث من حقيقة أن الثقة هي حجر الزاوية في أي نظام صحي (2). فبدون ثقة المريض في أن معلوماته الحساسة ستُعامل بسرية وأمان، قد يحجم عن مشاركة معلومات ضرورية للتشخيص الدقيق، أو قد يتجنب استخدام الأدوات الرقمية التي يمكن أن تحسن من صحته (3). وبالتالي، فإن حماية البيانات الصحية ليست مجرد التزام قانوني أو تقني، بل هي ضرورة أساسية لضمان استدامة وفعالية منظومة الصحة الرقمية بأكملها، والحفاظ على العلاقة الجوهرية بين المريض ومقدم الرعاية.

لمعالجة هذه الإشكالية، يتبع هذا البحث منهجاً تحليلياً مقارناً، حيث يقوم بتحليل طبيعة البيانات الصحية الرقمية ومخاطرها، ثم يقارن بين الأطر التنظيمية المختلفة، ويستعرض الحلول التقنية المتاحة. وينقسم هيكل الورقة إلى ثلاثة مباحث رئيسية؛ يتناول المبحث الأول ماهية البيانات الصحية في البيئة الرقمية وأبعادها المختلفة. ويستعرض المبحث الثاني المخاطر المتعددة التي تحدق بهذه البيانات، من التهديدات السيبرانية إلى التحديات الأخلاقية. أما المبحث الثالث، فيركز على استعراض الأطر القانونية والتقنية التي تشكل خط الدفاع لحماية هذه البيانات. وأخيراً، تقدم الخاتمة خلاصة للنتائج التي تم التوصل إليها، مع مجموعة من التوصيات الموجهة لمختلف الأطراف الفاعلة في هذا المجال.

1- ماهية البيانات الصحية في البيئة الرقمية وأبعادها

لفهم تحديات حماية البيانات الصحية الرقمية، لا بد أولاً من تفكيك ماهية هذه البيانات وتحديد أبعادها المتشعبة. لم تعد "البيانات الصحية" تقتصر على الملف الطبي المحفوظ في عيادة الطبيب، بل تحولت إلى بصمة رقمية ديناميكية وشاملة، تجمع بين المعلومات السريرية والبيانات التي يولدها المريض بنفسه، لتشكل صورة متكاملة ليس فقط عن حالته المرضية، بل عن نمط حياته وسلوكياته. يستعرض هذا المبحث تعريف هذه البيانات وأنواعها، والمنصات التي تجمعها، والاستخدامات المزدوجة التي تزيد من تعقيد حمايتها.

1-1- تعريف البيانات الصحية الرقمية وأنواعها وحساسيتها

يمكن تعريف البيانات الصحية الرقمية بشكل واسع بأنها أي معلومة تتعلق بالحالة الصحية الجسدية أو العقلية الماضية أو الحالية أو المستقبلية لفرد معين، والتي يمكن من خلالها تحديد هوية ذلك الفرد بشكل مباشر

أو غير مباشر (4). وتتجاوز هذه البيانات مجرد التشخيصات الطبية لتشمل طيفاً واسعاً من المعلومات التي يمكن تصنيفها على النحو التالي:

- البيانات السريرية: وهي البيانات التي يتم إنشاؤها في سياق الرعاية الصحية التقليدية، وتشمل التاريخ الطبي للمريض، نتائج الفحوصات المخبرية، صور الأشعة، التشخيصات، خطط العلاج، والأدوية الموصوفة.
- البيانات التي ينشئها المريض (Patient-Generated Health Data - PGHD): وهي فئة متنامية من البيانات التي يجمعها الأفراد بأنفسهم، غالباً خارج البيئة السريرية، باستخدام تطبيقات الصحة واللياقة البدنية والأجهزة القابلة للارتداء. وتوضح واجهات برمجة التطبيقات مثل Google Fit مدى دقة وحساسية هذه البيانات، حيث يمكنها جمع معلومات عن معدل نبضات القلب، ومستوى الجلوكوز في الدم، وضغط الدم، وأنماط النوم، ونسبة تشبع الأكسجين في الدم، والوزن، وحتى بيانات شديدة الخصوصية تتعلق بالصحة الإنجابية للمرأة (5).
- البيانات الوراثية والبيو مترية: وتعتبر من أكثر أنواع البيانات حساسية على الإطلاق، حيث تشمل بيانات الحمض النووي (DNA) والجينوم البشري الكامل، والتي لا تكشف فقط عن الحالة الصحية الحالية للفرد، بل عن استعداده الجيني لأمراض مستقبلية، وقد تمتد آثارها لتشمل أقاربه البيولوجيين (6).
- البيانات الإدارية والمالية: وتشمل معلومات الفواتير، أرقام الحسابات المصرفية، تفاصيل بطاقات الائتمان، ومعلومات التأمين الصحي، والتي تربط هوية الفرد المالية بخدمات الرعاية الصحية التي يتلقاها.

من منظور هيكلي، يمكن تصنيف هذه البيانات إلى بيانات منظمة (Structured Data) وبيانات غير منظمة (Unstructured Data). البيانات المنظمة هي بيانات موحدة وسهلة المعالجة آلياً، أما البيانات غير المنظمة، فهي تفتقر إلى نموذج بيانات محدد مسبقاً. وتشير التقديرات إلى أن البيانات غير المنظمة تشكل الغالبية العظمى من البيانات الصحية (حوالي 60% في الولايات المتحدة عام 2013)، مما يمثل تحدياً كبيراً أمام جهود تحليلها وحمايتها بشكل فعال (7).

إن هذا التنوع والعمق في البيانات المجمعة يقودنا إلى استنتاج جوهري: لقد حدث تحول نوعي في طبيعة البيانات الصحية، من كونها "بيانات رعاية صحية" مرتبطة بلحظات المرض، إلى كونها "بيانات حياة" مستمرة. في النموذج التقليدي، كانت البيانات الصحية محصورة في سياق سريري متقطع، كزيارة للطبيب أو الإقامة في المستشفى. أما اليوم، فإن تطبيقات الصحة الرقمية والأجهزة القابلة للارتداء تجمع بيانات على مدار الساعة، لا تعكس فقط "المرض" بل "نمط الحياة" اليومي. وعندما يتم دمج هذه البيانات الصحية المستمرة مع أنواع أخرى من البيانات الرقمية، فإنها لا تشكل مجرد سجل صحي، بل "بصمة رقمية سلوكية" شاملة ودقيقة للفرد. هذا التحول يرفع من مستوى الخطورة بشكل هائل؛ فالاختراق لم يعد يهدد بكشف مرض معين فحسب، بل يهدد

بكشف أدق تفاصيل حياة الفرد الخاصة، مما يفتح الباب أمام أشكال جديدة من التمييز في مجالات التوظيف، والتأمين، والإقراض، وحتى إمكانية التلاعب السلوكي.

1-2- منصات الصحة الرقمية: السجلات الصحية الإلكترونية وتطبيقات الصحة المتنقلة

تُجمع البيانات الصحية الرقمية وتُدار وتُشارك عبر مجموعة متنوعة من المنصات، لكل منها خصائصها ووظائفها التي تؤثر على كيفية حمايتها. ويمكن التمييز بين الفئات الرئيسية التالية:

- السجلات الطبية الإلكترونية (Electronic Medical Records - EMRs): هي النسخ الرقمية للسجلات الورقية التقليدية، وتعمل كنظام داخلي ضمن منشأة صحية واحدة، وهي ليست مصممة للمشاركة خارج حدود المنشأة (8).
- السجلات الصحية الإلكترونية (Electronic Health Records - EHRs):تمثل تطوراً أكثر شمولاً، حيث تم تصميمها لتوفير نظرة شاملة ومتكاملة على صحة المريض، وقابلة للتشغيل البيني (Interoperable) بين مختلف مقدمي الرعاية الصحية المصرح لهم.
- السجلات الصحية الشخصية(Personal Health Records - PHRs): هي سجلات صحية يديرها المريض بنفسه، وغالباً ما يتم الوصول إليها عبر "بوابة المريض" (Patient Portal) التي توفرها المؤسسة الصحية.
- تطبيقات الصحة المتنقلة (mHealth):تشكل هذه الفئة نظاماً بيئياً ضخماً وسريع النمو، حيث قُدر عددها بحوالي 300,000 تطبيق في عام 2017، مع توقع نمو سنوي بنسبة 25% (9). ورغم فوائدها، تواجه هذه التطبيقات تحديات فريدة تتعلق بقابلية الاستخدام، وجودة المعلومات، ووجود نقص كبير في الإرشادات الأمنية الموجهة للمطورين (10).

إن هذا التطور في منصات جمع البيانات يعكس انتقالاً من "نظام مغلق" إلى "نظام بيئي مفتوح"، وهو ما يوسع محيط التهديد الأمني بشكل هائل. في عصر السجلات الطبية الإلكترونية (EMR)، كان محيط الأمان محدداً وواضحاً نسبياً.

مع ظهور السجلات الصحية الإلكترونية (EHR)، توسع هذا المحيط ليشمل شبكة من المؤسسات المترابطة. أما ظهور السجلات الصحية الشخصية (PHR) وتطبيقات الصحة المتنقلة (mHealth)، فقد نقل نقطة الضعف النهائية إلى يد المستخدم مباشرةً. لم تعد مسؤولية الأمن تقع على عاتق مؤسسة واحدة، بل أصبحت مسؤولية مشتركة وموزعة بين المريض، ومطور التطبيق، ومزود الخدمة السحابية، ومقدم الرعاية الصحية. هذا التوزيع المعقد للمسؤولية يخلق ما يمكن تسميته بـ "فجوات المساءلة" (Accountability Gaps)، حيث يصبح من الصعب في حالة حدوث خرق أمني تحديد المسؤول بشكل قاطع.

1-3- الاستخدامات المزدوجة للبيانات الصحية وتضارب المصالح

تزداد قيمة البيانات الصحية بشكل كبير عندما يتم استخدامها لأغراض تتجاوز الرعاية المباشرة للمريض. هذا الاستخدام المزدوج يخلق فرصاً هائلة للتقدم الطبي، ولكنه يثير في الوقت نفسه تساؤلات جدية حول تضارب المصالح والموافقة. يمكن التمييز بوضوح بين نوعين من الاستخدام:

- الاستخدام الأولي (Primary Use): هو الغرض الأساسي الذي تُجمع من أجله البيانات، وهو تقديم الرعاية الصحية المباشرة للفرد.
- الاستخدام الثانوي (Secondary Use): يشمل أي استخدام للبيانات خارج نطاق تقديم الرعاية المباشرة، مثل البحث العلمي، دراسات الصحة العامة، وتحليلات البيانات الضخمة (11).

إن القيمة الاقتصادية الهائلة للبيانات الصحية تكمن بشكل أساسي في استخدامها الثانوي المجمع. وقد أدى ذلك إلى دخول شركات التكنولوجيا الكبرى بقوة إلى قطاع الرعاية الصحية، في ظاهرة أطلق عليها البعض "أمركة الرعاية الصحية" أو "Googlization of Healthcare" (12). تعتمد نماذج الأعمال لهذه الشركات بشكل أساسي على جمع ومعالجة كميات هائلة من البيانات لتوليد رؤى وتقديم خدمات مخصصة. هذا الواقع يخلق تضارباً جوهرياً في المصالح؛ فبينما يكون هدف مقدم الرعاية الصحية هو خدمة المريض، قد يكون الهدف الأساسي لشركة التكنولوجيا هو تحقيق الربح من بيانات هذا المريض.

هذا الوضع يضعنا أمام معضلة أخلاقية وقانونية عميقة. يمكن القول إن البيانات الصحية قد أصبحت "النفط الجديد" (13)، ونقطة الخلاف الجوهرية تكمن في تحديد من يملك حقوق استخراج هذا "النفط" وتكريره والاستفادة منه. إن الإجابة على هذا السؤال الجوهري ليست مجرد نقاش فلسفي، بل هي التي سترسم ملامح الجيل القادم من تشريعات الصحة الرقمية، وتحدد التوازن بين تشجيع الابتكار وحماية الحقوق الأساسية للأفراد.

2- المخاطر المحدقة بالبيانات الصحية للمرضى في تطبيقات الصحة الرقمية

مع تزايد حجم البيانات الصحية الرقمية وتعدد نقاط جمعها ومعالجتها، تتسع دائرة المخاطر التي تهدد سريتها وسلامتها وتوافرها. لا تقتصر هذه المخاطر على الهجمات السيبرانية الخارجية التي تتصدر العناوين، بل تمتد لتشمل ثغرات كامنة في بنية التطبيقات نفسها، ومخاطر غير مباشرة تنشأ من شبكة الأطراف الثالثة المعقدة، بالإضافة إلى تحديات أخلاقية وقانونية عميقة تفرضها التقنيات الحديثة مثل الذكاء الاصطناعي. يستعرض هذا المبحث هذه المخاطر بشكل مفصل، كاشفاً عن طبيعتها المتشابكة وتأثيراتها المحتملة على المرضى والمنظومة الصحية.

2-1- تهديدات الأمن السيبراني في قطاع الرعاية الصحية

أصبح قطاع الرعاية الصحية هدفاً رئيسياً لمجرمي الإنترنت، نظراً للقيمة العالية للبيانات الصحية في الأسواق السوداء، والطبيعة الحرجة للخدمات التي يقدمها القطاع، مما يجعله أكثر عرضة للابتزاز. يمكن تصنيف أبرز تهديدات الأمن السيبراني على النحو التالي:

- برامج الفدية (Ransomware): تعد من أخطر الهجمات وأكثرها تأثيراً. يقوم المهاجمون بتشفير أنظمة المستشفيات الحيوية، ثم يطالبون بفدية مالية ضخمة مقابل مفتاح فك التشفير. تعتبر المستشفيات هدفاً مثالياً لهذه الهجمات لأن أي توقف في خدماتها يهدد حياة المرضى بشكل مباشر (14). ويعد هجوم "WannaCry" العالمي في عام 2017 مثالاً صارخاً على التأثير المدمر لهذه البرامج، حيث أثر على أكثر من 200 ألف جهاز كمبيوتر في أكثر من 100 دولة وكلف ما يقدر بنحو 8 مليارات دولار (15).
- التصيد الاحتيالي (Phishing): هي هجمات تعتمد على الهندسة الاجتماعية لخداع الموظفين أو المرضى ودفعهم إلى الكشف عن بيانات اعتماد الدخول الخاصة بهم. وتتطور هذه الهجمات لتصبح أكثر استهدافاً، مثل "التصيد الاحتيالي بالرمح" (Spear Phishing) أو "تصيد الحيتان" (Whale Phishing) (16).
- البرمجيات الخبيثة (Malware): مصطلح واسع يشمل الفيروسات، وأحصنة طروادة (Trojans)، وبرامج التجسس (Spyware)، وتهدف إلى سرقة البيانات أو تعطيل العمليات.
- هجمات حجب الخدمة الموزعة (DDoS): تهدف هذه الهجمات إلى إغراق خوادم المستشفى بحركة مرور زائفة لجعلها غير متاحة للمستخدمين الشرعيين.

إن ما يميز الهجمات السيبرانية في قطاع الرعاية الصحية عن غيرها من القطاعات هو أن تأثيرها يتجاوز الخسارة المالية. فإن الهجوم السيبراني ليس مجرد جريمة بيانات، بل هو تهديد مباشر للصحة العامة والسلامة الجسدية (17). لهذا السبب، يجب إعادة تصنيف الهجمات السيبرانية التي تستهدف البنية التحتية الصحية الحيوية، من كونها مجرد "جرائم إلكترونية" إلى اعتبارها "أعمالاً تهدد السلامة العامة".

2-2- تحديات تطبيقات الصحة المتنقلة (mHealth) ومخاطر الطرف الثالث

بينما تواجه المؤسسات الصحية الكبيرة تهديدات منظمة، فإن النظام البيئي لتطبيقات الصحة المتنقلة (mHealth) يطرح مجموعة مختلفة من المخاطر التي غالباً ما تكون أقل وضوحاً ولكنها لا تقل خطورة. يمكن تقسيم هذه المخاطر إلى ثلاث فئات رئيسية:

- مخاطر متعلقة بالتطبيق نفسه: العديد من تطبيقات الصحة المتنقلة تعاني من مشاكل جوهرية، مثل رداءة جودة المعلومات وعدم دقتها، والافتقار إلى التحقق العلمي (18). كما أن العديد من المطورين يفتقرون إلى الخبرة أو الموارد اللازمة لتطبيق ممارسات أمنية قوية، وهناك نقص عام في الإرشادات والمعايير الأمنية الواضحة الموجهة لهم (19).
- مخاطر متعلقة ببيئة التشغيل: يعتمد أمان هذه التطبيقات على البيئة التي تعمل فيها، مثل ضعف الاتصال بالإنترنت أو استخدام أجهزة وأنظمة تشغيل قديمة.
- مخاطر الطرف الثالث (Third-Party Risk): تمثل هذه الفئة واحدة من أكبر نقاط الضعف الخفية. يعتمد المطورون على شبكة معقدة من الموردين ومزودي الخدمات السحابية. وتشير التقديرات إلى أن حوالي 60% من جميع خروقات البيانات تنطوي على طرف ثالث، والعديد من المؤسسات تفتقر إلى

معايير أمان صارمة مطبقة على هؤلاء البائعين (20).

إن هذا الاعتماد الكبير على أطراف ثالثة يخلق "سلسلة ثقة" طويلة وهشة، حيث تحدد أضعف حلقة في هذه السلسلة قوة السلسلة بأكملها. لم يعد كافياً أن يقوم المستخدم بتقييم سياسة الخصوصية للتطبيق الذي يستخدمه مباشرة، فالمخاطر الحقيقية قد تكون مخفية في طبقات أعمق من سلسلة التوريد الرقمية التي لا يراها المستخدم.

2-3- الأبعاد الأخلاقية والقانونية لمعالجة البيانات بالتقنيات الحديثة

إلى جانب التهديدات التقنية، يثير استخدام التقنيات المتقدمة، وعلى رأسها الذكاء الاصطناعي (AI)، في تحليل البيانات الصحية مجموعة من المعضلات الأخلاقية والقانونية العميقة التي تتحدى الأطر التقليدية للمسؤولية والإنصاف.

- التحيز الخوارزمي (Algorithmic Bias): يمكن لنماذج الذكاء الاصطناعي أن تعكس وتضخم التحيزات الموجودة في البيانات التي تدربت عليها، مما يؤدي إلى تشخيصات غير دقيقة ويفاقم الفوارق الصحية القائمة (21).
- الشفافية وقابلية التفسير (Transparency and Explainability): تعمل العديد من نماذج الذكاء الاصطناعي المتقدمة كـ "صناديق سوداء" (Black Boxes)، حيث من الصعب فهم المنطق الذي أدى بها إلى قرار معين، مما يتحدى مبدأ المساءلة (22).
- المسؤولية والمساءلة (Responsibility and Accountability): تطرح هذه القضية سؤالاً جوهرياً: في حالة حدوث خطأ تشخيصي من قبل نظام ذكاء اصطناعي، من هو المسؤول قانونياً؟ هل هو المطور، أم المستشفى، أم الطبيب؟ (23).
- الموافقة المستنيرة (Informed Consent): كيف يمكن الحصول على موافقة مستنيرة حقيقية من المريض لمعالجة بياناته باستخدام الذكاء الاصطناعي، عندما تكون طبيعة المعالجة نفسها معقدة للغاية؟

يمكن الاستعانة بأطر مثل "مبادئ أخلاقيات الذكاء الاصطناعي" الصادرة عن الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA) لتحليل هذه القضايا، والتي تؤكد على قيم مثل النمو الشامل، القيم الإنسانية والعدالة، الشفافية، المتانة والأمن، والمسؤولية والمساءلة (24). إن الذكاء الاصطناعي في قطاع الصحة لا يغير فقط "كيفية" إجراء التشخيص، بل يغير "طبيعة" المعرفة الطبية والمسؤولية المهنية، مما يتطلب إعادة تعريف شاملة لمعايير الممارسة الطبية والمسؤولية القانونية.

3- الأطر القانونية والتقنية لحماية البيانات الصحية الرقمية

بعد تشخيص الطبيعة المعقدة للبيانات الصحية الرقمية والمخاطر المتعددة التي تواجهها، ينتقل هذا المبحث إلى استعراض خطوط الدفاع والحلول المتاحة. إن حماية هذه البيانات لا يمكن أن تتم من خلال حل واحد، بل تتطلب نهجاً متكاملاً ومتعدد الطبقات يجمع بين الأطر التشريعية الرصينة التي تحدد الحقوق

والواجبات، والضمانات التقنية والإجرائية التي تشكل الحماية العملية، بالإضافة إلى استشراف دور التقنيات الناشئة التي قد تقدم حلولاً مبتكرة للتحديات المستقبلية.

3-1- الأطر التشريعية لحماية البيانات: دراسة مقارنة

تعتبر التشريعات والقوانين حجر الزاوية في حماية البيانات، حيث تضع القواعد الأساسية التي يجب على جميع الأطراف الالتزام بها. على الصعيد العالمي، برزت عدة نماذج تشريعية رائدة، وسنقوم هنا بمقارنة ثلاثة من أبرزها في سياق حماية البيانات الصحية:

- اللائحة العامة لحماية البيانات (GDPR) – الاتحاد الأوروبي: دخلت حيز التنفيذ في عام 2018، وتعتبر المعيار الذهبي العالمي لحماية البيانات. تتميز بنطاق تطبيقها الواسع الذي يتجاوز الحدود الجغرافية، وتعرف البيانات الصحية كـ "فئة خاصة من البيانات الشخصية" تتطلب موافقة صريحة وحماية مشددة، مع فرض عقوبات مالية رادعة (25).
- قانون إخضاع التأمين الصحي لقابلية النقل والمساءلة (HIPAA) – الولايات المتحدة: صدر في عام 1996، وهو قانون قطاعي يركز على حماية "المعلومات الصحية المحمية" (PHI) داخل الولايات المتحدة. يفرض القانون مجموعة مفصلة من الضوابط الإدارية والتقنية والمادية، ولكنه أقل صرامة من GDPR في بعض الجوانب مثل متطلبات الموافقة وفترة الإبلاغ عن الخروقات (26).
- نظام حماية البيانات الشخصية (PDPL) – المملكة العربية السعودية: يمثل هذا النظام خطوة مهمة نحو مواءمة المملكة مع أفضل الممارسات الدولية، ويظهر تأثراً واضحاً بمبادئ GDPR. يمنح النظام أصحاب البيانات حقوقاً أساسية ويفرض التزامات واضحة على "جهات التحكم" و"جهات المعالجة"، ويشترط الحصول على موافقة صريحة لمعالجة البيانات الحساسة (27).

إن نقل البيانات عبر الحدود يخضع لقيود صارمة بموجب هذه التشريعات، خاصة GDPR وPDPL، حيث لا يسمح بالنقل إلا للدول التي توفر مستوى حماية "كافياً" أو باستخدام ضمانات أخرى مثل البنود التعاقدية القياسية (28). هذا الواقع يدفع الشركات العالمية إلى تبني استراتيجية امتثال موحدة تعتمد على "أعلى معيار مشترك" لتقليل المخاطر القانونية.

3-2- الضمانات التقنية والإجرائية لحماية البيانات

لا تكفي التشريعات وحدها لحماية البيانات؛ فلا بد من ترجمتها إلى ضوابط وإجراءات تقنية ملموسة. ومن أهم هذه الضمانات:

- التشفير (Encryption): هو عملية تحويل البيانات إلى نص مشفر غير مفهوم لا يمكن فكه إلا بمفتاح خاص. يجب تطبيقه على البيانات في جميع حالاتها: أثناء التخزين وأثناء النقل (29).
- ضوابط الوصول (Access Control): تهدف إلى ضمان عدم تمكن أي شخص من الوصول إلى البيانات إلا إذا كان مصرحاً له بذلك، بناءً على مبدأ " الحاجة إلى المعرفة" و"الحد الأدنى من الامتيازات"

.(30)

- إخفاء الهوية وإزالة تحديدها (Anonymization & De-identification): هي تقنيات تهدف إلى إزالة معلومات التعريف الشخصية من مجموعة البيانات للسماح بمشاركتها لأغراض البحث مع الحفاظ على الخصوصية. تشمل هذه التقنيات نماذج مثل k-anonymity وl-diversity (31).
- الخصوصية حسب التصميم (Privacy by Design - PbD): هي فلسفة شاملة ومنهجية استباقية تقوم على سبعة مبادئ أساسية، أهمها أن تكون الخصوصية "استباقية وليست رد فعل"، و"مدمجة في التصميم منذ البداية"، وأن تكون "الإعداد الافتراضي" للنظام (32).

إن الحماية الفعالة تتطلب تبني نهج "الدفاع في العمق" (Defense-in-Depth)، وهو استراتيجية أمنية متعددة الطبقات تجمع بين هذه الضوابط التقنية، بالإضافة إلى التدريب والتوعية المستمرة للموظفين لخلق ثقافة أمنية قوية.

3-3- دور التقنيات الناشئة في تعزيز الأمن والخصوصية

في مواجهة التحديات المتزايدة، تقدم التقنيات الناشئة حلولاً واعدة يمكن أن تعيد تشكيل مشهد أمن وخصوصية البيانات الصحية.

- تقنية البلوك تشين (Blockchain): تمتلك هذه التقنية القدرة على إحداث ثورة في طريقة إدارة السجلات الصحية. فبدلاً من تخزين البيانات في قواعد بيانات مركزية، تسمح البلوك تشين بإنشاء سجلات لامركزية وموزعة وثابتة (Immutable). الأهم من ذلك، يمكن للبلوك تشين أن تمنح المرضى سيطرة حقيقية على بياناتهم من خلال استخدام "المفاتيح" الخاصة لمنح أو حجب الوصول، مما يحقق نموذجاً حقيقياً للوصول المتحكم فيه من قبل المريض (33).
- الذكاء الاصطناعي للأمن (AI for Security): يمكن تسخير الذكاء الاصطناعي لتعزيز الدفاعات السيبرانية من خلال تحليل كميات هائلة من بيانات الشبكة في الوقت الفعلي واكتشاف السلوكيات الشاذة التي قد تشير إلى هجوم سيبراني.
- الحوسبة الحافظة للخصوصية (Privacy-Preserving Computation): هي مجموعة من التقنيات المتقدمة التي تسمح بإجراء عمليات حسابية وتحليلية على البيانات دون الكشف عن محتوى البيانات نفسها، ومن أمثلتها التشفير المتماثل (Homomorphic Encryption) والحساب الآمن متعدد الأطراف (Secure Multi-Party Computation) (34).

إن هذه التقنيات الناشئة تحمل في طياتها وعداً بالانتقال من نموذج "الحماية" إلى نموذج "التمكين"، حيث يصبح المريض هو "حارس بوابة" بياناته، وليس المؤسسة. ورغم أن هذا التحول واعد، إلا أنه يواجه تحديات تتعلق بقابلية التوسع والتكلفة والتشغيل البيني.

الخاتمة: النتائج والتوصيات:

بعد التحليل المعمق لمختلف جوانب حماية البيانات الصحية للمرضى في ظل تطبيقات الصحة الرقمية، يمكن استخلاص مجموعة من النتائج الجوهرية وتقديم توصيات عملية لمختلف الأطراف المعنية، بهدف بناء منظومة صحية رقمية آمنة وموثوقة.

أولاً: النتائج

لقد كشف البحث أن قضية حماية البيانات الصحية الرقمية ليست مجرد تحدٍ تقني، بل هي إشكالية معقدة ومتعددة الأبعاد. وتتمثل أبرز النتائج فيما يلي:

1. تحول طبيعة البيانات وارتفاع مستوى المخاطر: لقد تطورت البيانات الصحية الرقمية من سجلات سريرية متقطعة إلى بصمة سلوكية وحياتية شاملة ومستمرة، مما يرفع من مخاطر انتهاك الخصوصية إلى مستوى غير مسبوق.
2. تعقيد النظام البيئي وفجوات المساءلة: إن النظام البيئي للصحة الرقمية، بفضل انتشاره وتعقيده، يخلق "فجوات مساءلة" كبيرة، حيث تصبح مسؤولية حماية البيانات ضائعة بين مختلف الأطراف.
3. التهديد السيبراني كخطر على السلامة الجسدية: لقد أظهر التحليل أن الهجمات السيبرانية على قطاع الرعاية الصحية تتجاوز كونها جرائم بيانات لتصبح تهديداً مباشراً للسلامة الجسدية للمرضى (35).
4. المعضلات الأخلاقية للتقنيات الحديثة: يطرح استخدام الذكاء الاصطناعي تحديات أخلاقية وقانونية عميقة تتعلق بالتحيز، والشفافية، والمسؤولية، مما يتطلب تطوير أطر حوكمة جديدة (36).
5. الحاجة إلى نهج شمولي ومتعدد الطبقات: إن الحماية الفعالة تتطلب بالضرورة تبني نهج "الدفاع في العمق"، الذي يدمج بين الأطر التشريعية القوية، والضوابط التقنية المتينة، وتنمية ثقافة تنظيمية واعية.

ثانياً: التوصيات

بناءً على النتائج المستخلصة، يمكن تقديم التوصيات العملية التالية الموجهة لمختلف الأطراف الفاعلة:

1. لصناع السياسات والجهات التنظيمية:

- تحديث وتطوير التشريعات: ضرورة المراجعة الدورية وتحديث التشريعات الحالية لحماية البيانات لتواكب نماذج البيانات الجديدة والمخاطر الناشئة (37).
- حوكمة الذكاء الاصطناعي: وضع أطر تنظيمية واضحة وملزمة لاستخدام الذكاء الاصطناعي في الرعاية الصحية.
- تعزيز التعاون الدولي: تشجيع التعاون بين الدول لوضع معايير دولية موحدة وتنسيق الجهود في مكافحة الجرائم السيبرانية.

2. لمؤسسات الرعاية الصحية:

- تبني "الخصوصية حسب التصميم": جعل مبادئ "الخصوصية حسب التصميم" (PbD) سياسة إلزامية

ومحوراً أساسياً في جميع العمليات.

- الاستثمار في العنصر البشري: الاستثمار بكثافة في برامج التدريب والتوعية المستمرة لجميع الموظفين حول مخاطر الأمن السيبراني (38).
- تدقيق سلسلة التوريد: تطبيق إجراءات تدقيق وفحص صارمة على جميع موردي الطرف الثالث والشركاء التقنيين.

3. لمطوري التطبيقات وشركات التكنولوجيا:

- تأمين دورة حياة التطوير: دمج الأمن والخصوصية في كل مرحلة من مراحل تطوير البرمجيات.
- الشفافية وبناء الثقة: زيادة الشفافية مع المستخدمين بشأن ممارسات جمع البيانات من خلال سياسات خصوصية واضحة وموجزة (39).
- تمكين المستخدم: تطوير أدوات تحكم تمنح المستخدمين سيطرة دقيقة وحقيقية على بياناتهم.

4. للمرضى والمستخدمين:

- رفع الوعي بالحقوق: يجب على الأفراد السعي لمعرفة حقوقهم بموجب قوانين حماية البيانات في بلدانهم.
- التثقيف الذاتي حول الممارسات الآمنة: تعلم وتطبيق الممارسات الرقمية الأساسية، مثل استخدام كلمات مرور قوية وتفعيل المصادقة الثنائية.

الهوامش:

(1) Bächle, T.C., & Wernick, A. (2019). The Futures of E-Health. Social, Ethical and Legal Challenges. Berlin : Humboldt Institute for Internet and Society.

(2) Aumet. (2025). خصوصية البيانات الطبية وتحديات الأمن السيبراني.

(3) Medicover Hospitals. (n.d.). Secure Health Data : Protecting Privacy in Digital Age.

(4) مجلة روح القوانين. (د.ت.). حماية البيانات الشخصية الطبية الحساسة.

(5) Google Developers. (د.ت). Health data types.

(6) مجلة روح القوانين. (د.ت.). حماية البيانات الشخصية الطبية الحساسة.

(7) ويكيبيديا. (د.ت.). البيانات الصحية.

(8) Medoc. (د.ت). Electronic Medical Records vs. Electronic Health Records.

(9) Malvey, D.M., & Slovensky, D.J. (2017). Global mHealth policy arena : status check and future directions. mHealth, 3, 41.

(10) Mendonca, E. A., et al. (2004). Major Challenges with Mobile Healthcare Applications.

(11) ويكيبيديا. (د.ت.). البيانات الصحية.

(12) Sharon, T. (2018). When digital health meets digital capitalism, how many common goods are at stake ? Big Data & Society, 5(2).

(13) مرزا، ياسمين. (د.ت.). إخراج القيمة من البيانات. مجلة الجودة الصحية.

(14) Aumet. (2025). خصوصية البيانات الطبية وتحديات الأمن السيبراني.

(15) بوابة الأهرام الاقتصادية. (2023). الهجمات السيبرانية الأكثر شيوعًا.

(16) RMG. (2021). أبرز أنواع الهجمات السيبرانية.

(17) مركز تريندز للبحوث والاستشارات. (2023). الأمن السيبراني في 2023: تحولات وتحديات عصرية.

(18) Stoyanov, S. R., et al. (2015). The effectiveness of mobile-health technology-based health behaviour change or disease management interventions for health care consumers : a systematic review. PLoS medicine, 10(1).

(19) Zubaydi, H. D., et al. (2021). Security and Privacy in mHealth Apps : A Review of the State of the Art. Journal of Medical Systems, 45(8).

(20) SVU Online. (د.ت.). Cybersecurity in the Modern Era.

(21) Moldovan, A., Vîscan, A., & Groșan, C. (2025). Algorithmic Bias in Healthcare AI : A Systematic Review of Implications and Mitigation. Proceedings of the International Conference on Enterprise Software Evaluation.

(22)الهيئة السعودية للبيانات والذكاء الاصطناعي) .(SDAIA) د.ت.). دليل أخلاقيات الذكاء الاصطناعي.

(23) Mendonca, E. A., et al. (2004). Major Challenges with Mobile Healthcare Applications.

(24)الهيئة السعودية للبيانات والذكاء الاصطناعي) .(SDAIA) د.ت.). دليل أخلاقيات الذكاء الاصطناعي.

(25) Censinet. (2025). GDPR vs. HIPAA : Key Differences for Healthcare.

(26) Stfalcon. (2024). A Comparative Analysis of GDPR and HIPAA Regulations.

(27) Trusted Vision. (2025). فهم نظام حماية البيانات الشخصية في المملكة العربية السعودية: دليل الامتثال.

(28) Proz.com. (د.ت.). نقل البيانات عبر الحدود.

(29) Faster Capital. (2025). حماية البيانات في العصر الرقمي.

(30) Maaz, M., et al. (د.ت.). Factors of Access Control Management in Electronic Healthcare : The Patients' Perspective.

(31) Li, M. (2023). PREDANO : A Privacy Enhancement Data Anonymization Platform for Medical Datasets. University of Zurich.

(32) Faster Capital. (2025). الخصوصية حسب التصميم: دمج إخفاء الهوية في عمليات جمع البيانات.

(33) App Master. (2024). دليل المبتدئين لفهم أمن وخصوصية السجلات الصحية الإلكترونية.

(34) Faster Capital. (2025). الخصوصية حسب التصميم: دمج إخفاء الهوية في عمليات جمع البيانات.

(35) Aumet. (2025). خصوصية البيانات الطبية وتحديات الأمن السيبراني.

(36) مؤتمر القمة العالمي للابتكار في الرعاية الصحية (ويش). (2024). تقرير يسلط الضوء على الأبعاد الأخلاقية لاستخدام الذكاء الاصطناعي في الرعاية الصحية.

(37) Bächle, T.C., & Wernick, A. (2019). The Futures of E-Health. Social, Ethical and Legal Challenges. Berlin : Humboldt Institute for Internet and Society.

(38) Aumet. (2025). خصوصية البيانات الطبية وتحديات الأمن السيبراني.

(39) Sedik, A., et al. (2021). Digital Privacy of Users of Deepfake Applications.