# الحماية الجنائيّة للسجلات الطبيّة الرقميّة "دراسة مقارنة"

**د. عمر عبد المجيد مصبح**
**جامعة السلطان قابوس**

**د. سيف إبراهيم المصاروة**
**جامعة مؤته**

## الملخص

تتناول هذه الدراسة موضوع الحماية الجنائيّة للسجلات الطبيّة الرقميّة "دراسة مقارنة"، فقد باتت الميزة الأهم في نطاق الخدمات الصحيّة السجلات الرقميّة، إذ سعت هذه الدراسة إلى إبراز دور التقنيات المعلوماتية وتوظيفها في قطاع حسّاس كالقطاع الصحيّ، الذي يتطلب وضع نصوص قانونيّة تضمن سلامة وخصوصية المعطيات الطبيّة وسرّيّتها وطرق تبادلها وعدم الاعتداء عليها، تحقيقاً لاستخدامها بصفة سليمة وآمنة، ولحماية حقوق الشخص المعني بالمعطيات الطبيّة.

وخلصت الدراسة إلى جملة من المقترحات أهمها: أن يقوم المُشَرِّعان الأردني والعُماني بتنظيم تبادل معلومات وبيانات المرضى الرقميّة وجمعها وتخزينها وتسجيلها وحفظها واستعمالها وغيرها من الإجراءات، فضلاً عن قيام المُشَرِّع الأردني بفرض السرية على هذه المعلومات والبيانات، وحماية حقوق الشخص المعني بالمعالجة الطبيّة، وذلك بتجريم صور الاعتداء على المعلومات والبيانات الطبيّة والصحيّة كافة.

**الكلمات الدالة:** سجلات طبيّة، حماية جنائيّة، الرقميّة، السرية، الخصوصية.

# Criminal protection of digital medical records "A comparative study"

## Abstract

This study addressed criminal protection of digital medical records. Criminal protection has become the most important characteristic in the domain of health services and digital records. The current study aimed to demonstrate the role of information technology and its employment in a sensitive sector, such as the health sector which requires setting legal texts to ensure the safety, confidentiality, and specificity of medical requirements. Such legal texts should protect digital medical records against violation and secure their exchange methods in order to use them safely. They also protect the rights of those concerned with medical requirements.

The study concluded that there is a necessity of urging the Jordanian and Omani legislators to organize the process of exchanging, collecting, storing and recording the patients' digital data, in addition to urging the Jordanian legislator to maintain the confidentiality of these data. It is necessary to protect the rights of the individuals concerned with medical treatment and to criminalize all forms of violation against health and medical data.

**Key words:** medical records, criminal protection, digitalization, confidentiality, privacy.

## المقدمة

يمتاز عصرنا الحالي بتوافر المعطيات والبيانات، وزيادة استخدامنا لها، ويتجلى ذلك بصورة واضحة في زيادة الاعتماد على الشبكة العنكبوتية كمنهج للإدارة المعاصرة، وهذا ما يطلق عليه بالإدارة الإلكترونيّة، فلقد بات الاعتماد الواسع على أنظمة السجلات الطبيّة الإلكترونيّة (EMR) يُمكِّن الباحثين والمختصين من استخراج كميات هائلة من بيانات المرضى، والبحث عن أفضل التنبؤات بالنتائج الصحيّة،وفضلاً عن ذلك ترتبط كل أعمال الرعاية الطبيّة بمدى توافر المعطيات الطبيّة الدقيقة عن الحالة الصحيّة للمريض[1].

وتأسيساً على ما تقدم، فإن "الصحة الرقميّة"التي تتضمن إقحام التقنيات المعلوماتية من أجل رقمنة قطاع الصحة باعتبار أنّ هذه التكنولوجيات تعد بمثابة محرك وقيمة مضافة للقطاع الطبيّ،التي تتطلع إلى أتمتة المعطيات المتعلقة بقطاع الصحة والبيانات الخاصة بالمرضى، من خلال وضع ملف إلكترونيّ خاص بهم، يتضمن كلّ ما له علاقة بصحتهم على شبكة المعلوماتية ويمكن العودة إليه في كل فحص لمتابعة حالتهم الصحيّة.

ولقد أدى الدمج المتزايد للتكنولوجيا في النطاق الطبيّ إلى زيادة الدقة في الرعاية الصحيّة؛ ومع ذلك، لا تزال هناك حاجة إلى إحراز تقدم في تدابير الحماية الجزائية للفضاء السيبرانيّ، لذا فإنّ تكرار خروقات البيانات في صناعة الرعاية الصحيّة آخذ في الارتفاع، وهي الآن من بين القطاعات الأكثر استهدافًا للهجمات الإلكترونيّة على المستوى الدولي.

وعليه، فإن البيانات التي يتم الولوج إليها من خلال قرصنة البيانات الصحيّة ذات أهمية خاصة للمجرمين،حيث يتم تضمين البيانات الطبيّة للمريض في الملف الطبيّ للمراجع باعتبار أنّ هذه السجلات تتضمن بيانات خاصة، مثل الاسم وتاريخ الميلاد والتأمين ومعلومات مقدم الرعاية الصحيّة، فضلاً عن البيانات الصحيّة والوراثية، فلا يمكن استعادة الخصوصية والسرية أو عكس الضرر النفسيّ والاجتماعيّ عند تعرض البيانات الخاصة للخطر.

(1) فايز النجار، نظم المعلومات الإدارية، دار الحامد للنشر والتوزيع،عمان، 2007، ص 99.

## مشكلة الدراسة:

مما لاشك فيه، أنّ الملفات الطبيّة الرقميّة باتت تحل تدريجياً محل السجلات الورقية، ممّا طرح مجموعة من الإشكالات التي حاول الفقه إلى جانب القضاء معالجتها،فالسبب الأكثر شيوعاً لانتهاكات السجلات الطبيّة هو الاعتداء على معلومات السجل الطبيّ الرقميّ. ومن هنا تتمحور الإشكالية الرئيسة للموضوع المعالج في هذه الدراسة، كالتالي، إلى أي حد استطاع المُشَرِّع توفير الحماية الجنائيّة لبيانات ومعلوماتالسجلات الطبيّة الرقميّة؟

فالملفات الطبيّة الرقميّة يمكن أنْ تكون تهديدًا استراتيجيًا لحق المرء في بياناته، بحيث صار الأمن السيبرانيّ في مقدمة أولويات أنظمة الرعاية الصحيّة، وتعدّ الجهات ذات الشأن هذه المعضلة على أنّها إشكالية خطيرة تتسبب في انتشار انتهاكات خطيرة لخصوصية وحقوق المرضى، ممّا يتطلب ضمان سلامة وخصوصية سجلات المرضى وبياناتهم الطبيّة وخاصة الحساسة منها جنائيّاً.

## هدف الدراسة:

تهدف هذه الدراسة إلى:

1- إبراز دور التقنيات المعلوماتية وتوظيفها في قطاع حسّاس كالقطاع الصحيّ،مما يتطلب وضع قواعد دقيقة تضمن الحفاظ على حقوق كل طرف وتحديد واجباته، وهذه القواعد تهم خاصية سلامة وأمن البيانات والمعطيات الطبيّة، وطرق تبادلها، وضمان سرّيّتها وموثوقيتها، تحقيقاً لاستخدامها بصفة سليمة وآمنة.

2- وصف الحالات الرئيسة المتعلقة بالحماية الجنائيّة لخصوصية أنظمة البيانات الرقميّة وإجراءات تسجيل المرضى المعتمدة على الحاسب الآلي، ووصف الأساليب المستخدمة حاليًا للتغلب على هذه الإشكالات.

3- بيان قدرة السجلات الطبيّة المحوسبة على توفير الحماية لسرية المعلومات الشخصية للمريض، والاستفادة منها كدليل في المحكمة في قضايا الأخطاء الطبيّة.

## أهمية الدراسة:

بات معلوماً أنّ غالبية الانتهاكات الإجرامية هي لجمع معلومات لانتحال الهوية أو للاحتيال على التأمين الطبيّ، فحالات الاعتداء تثير مخاوف على سلامة السجلات الطبيّة الإلكترونيّة، وإنّ عدداً من شركات التأمين تم مهاجمتها من قبل الجناة (الهاكرز) في السنوات الأخيرة في عدة وقائع منفصلة، ممّا عرض أكثر من (90) مليون سجل طبيّ للانتهاكات والاعتداءات الإجرامية[1].

ولذلك، تعد خصوصية المرضى وأمن معلوماتهم الإشكال الأكثر إلحاحًا أمام تبني السجلات المؤتمتة في المجال الطبيّ، وبالنظر إلى التشريعات الجزائية الحالية[2]، وخاصة المقارنة منها التي تبنت السجلات الطبيّة الرقميّة.

## منهج الدراسة:

تفرض علينا طبيّعة الدراسة الأخذ بأكثر من منهج، فقد تم تبني المنهج الوصفي في عرضنا للمفاهيم العامة للدراسة، ومقاربة مختلف جوانبه القانونيّة، وكذلك استخدام المنهج التحليلي الاستقرائي وذلك باستخدام تقنية تحليل النصوص وتفسيرها،وبما أنّ الدراسة مقارنة فقد شمل نطاق الدراسة القوانين ذات الصلة بالمعلومات الصحيّة في بلدان مختارة مثل: أمريكا والإتحاد الأوروبي وأندونيسيا، والأردن وعُمان والإمارات، وبعض التشريعات الأخرى ذات الصلة بموضوع الدراسة.

## خطة الدراسة

تأسيساً على ما سبق بيانه، وحتى نتمكن من ضبط عناصر هذه الدراسة، سنتناول الأحكام العامة للسجل الطبيّ الرقميّ وأهميته في مبحث أول، وتأطير الحماية الجنائيّة للسجلات الطبيّة الرقميّة في مبحث ثانٍ.

(1)Medical Records Management: Everything You Need to Know. https://www.accesscorp.com/blog/medical-records-management-overview[Accessed 23 June 2021].

(2) انظر: خليل خيرالله، تنظيم الملف الطبي الإلكتروني وحماية بياناته في إطار تطوير القطاع الصحي والخدمات الصحية،بحث منشور على الموقع الإلكتروني: https://www.lita-lb.org/images/publication/_____.pdf.

## المبحث الأول: الأحكام العامة للسجل الطبيّ الرقميّ وأهميته

سيتم دراسة هذا المبحث من خلال توضيح مدلول السجل الطبيّ الرقميّ وأهميته في مطلب أول، ثم مظاهر التنظيم القانونيّ للسجل الطبيّ الرقميّ في مطلب ثانٍ.

### المطلب الأول: مدلول السجل الطبيّ الرقميّ وأهميته

يُعدّ السّجل الإلكترونيّ[1] نظاماً لا ورقيّاً يعزز وسيلة الحصول على البيانات بشكل سلس لتصبح البيانات الصحيّة لكل مريض متاحة بسهولة أمام مقدمي الرعاية الصحيّة، ويشمل السجل الطبيّ الرقميّ جميع الإجراءات والأنشطة الطبيّة المقدمة للمريض، وهو مشابه للملف الورقي المستخدم في القطاع الصحيّ.

وللبحث في مدلول السجل الطبيّ الرقميّ وأهميته،يستلزم بيان المقصود به من خلال تعريفه، ومن ثم بيان أهمية الدور الذي يضطلع به في المؤسسات الصحيّة عامة ، والجانب الجنائيّ خاصة.

#### الفرع الأول: تعريف السجل الطبيّ الرقميّ

بادئ ذي بدء، ظهر مصطلح الصحة الرقميّة في أوائل القرن الحالي، وهو يتضمن اعتماد التكنولوجيا المعاصرة لنقل الرعاية الصحيّة إلى المجال الطبيّ، لذلك تتطلب الإدارة الفعالة للصحة الإلكترونيّة فريقًا متعدد التخصصات بما في ذلك الاتصالات السلكية واللاسلكية[2] والأجهزة وعلوم الحاسب الآلي لتمكين تبادل البيانات الطبيّة عبر مناطق جغرافية واسعة.

وعوداً على بدء، فقد عُرف السجل الطبيّ الرقميّ بأنّه[3]: (الخزن الإلكترونيّ للمعلومات وتوفرها بشكل فوري إلى الشخص المخول الذي يقوم بتوثيق المعلومات ويقلل من الأخطاء الطبيّة)، وعُرف أيضاً بأنه: (عبارة عن ملف إلكترونيّ

---

(1) عرف قانون المعاملات الإلكترونية العماني رقم 69/ 2008 السجل الإلكتروني في المادة (1) منه ، بأنه: "العقد أو القيد أو رسالة المعلومات التي يتم إنشاؤها أو تخزينها أو استخراجها و نسخها أو إرسالها أو إبلاغها أو تسلمها بوسائل إلكترونية على وسيط ملموس أو وسيط آخر ويكون قابلاً للتسلم بشكل يمكن فهمه". وعرفه قانون المعاملات الإلكترونية الأردني رقم (15) لسنة 2015 بموجب المادة (2) منه بأنه "رسالة المعلومات التي تحتوي على قيد أو عقد أو أي مستند أو وثيقة من نوع آخر يتم إنشاء أي منها أو تخزينها أو استخدامها أو إرسالها أو تبليغها أو تسليمها باستخدام الوسيط الإلكتروني".

(2) عبدالحميد بسيوني،الصحة الإلكترونية، ط1، دار الكتب العلمية للنشر والتوزيع، القاهرة، 2008 ، ص25.

(3) Waegemann, Peter(2003) **EHR vs. CPR vs. EMR**, Healthcare Informatics, The McGraw-Hill Companies. https://www.academia.edu.

يشتمل على بيانات ومعطيات صحيّة وتمريضية وإدارية تتضمن مختلف الجوانب المتعلقة بالوضع الصحيّ للمريض...)[1]. لذلك، يساعد القيد الطبيّ الإلكترونيّ في خزن وتنظيم وعرض البيانات ويساهم في تحسين الرعاية الصحيّة المقدمة للمرضى.

وقد استخدم لوصف النظم الآلية استناداً إلى الوثيقة المصورة أو البرامج التي تم تطويرها ضمن الأنشطة الصحيّة أو مراكز صحة المجتمع وقد استخدم بصورة واسعة من لدن المختصين في العديد من البلدان.

**الفرع الثاني: أهمية السجل الطبيّ الرقميّ صحيّاً وجنائيّاً**

بدأت بعض المشافي في استخدام التغييرات في نموذج السجل الطبيّ من التقليدي إلى الإلكترونيّ لسهولة الحصول على هذا النظام، وبات استخدام السجلات الطبيّة الرقميّة، كسجلات إدارية، وأدلة رقميّة للبحث في المستندات كدليل على توثيق الخدمات المقدمة للمرضى، ويعد السجل الطبيّ مستندًا أساسيًا؛ لأنّ جميع إجراءات الخدمة التي تم إجراؤها للمراجعين مسجلة فيه.

وأضحت المستشفيات تدرك بشكل متزايد أنّ السجلات الطبيّة الإلكترونيّة (EMR) لديها القدرة على تقديم كثير من المزايا، مثل تحسين خدمات الرعاية الطبيّة المقدمة للمرضى، وتقليل الأخطاء الطبيّة، وانخفاض التكاليف، وسنبين أهمية السجلات الطبيّة الرقميّة صحيّاً وجنائيّاً على النحو التالي:

**أولاً:أهمية السجلات الطبيّة الرقميّة للهيئات الصحيّة.**

يساعد هذا النوع من السجلات الرقميّة على التواصل بين مقدمي الرعاية الصحيّة ببساطة والوصول بمرونة إلى سجلات المرضى،مما يتيح لهم تقديم رعاية آمنة ودقيقة مع الاطلاع الكامل على ملف المريض [2]، ومن ثم حصوله على رعاية عالية الجودة، وهو ما سيلاحظه من خلال التواصل والتنسيق السريع بينه وبين فريق الرعاية الصحيّة فيما يتعلق بحالته الصحيّة وعلاجه.

---

(1) لمياء الخليفة، بناء نظام السجلات الطبية، بحث تكميلي لنيل درجة الماجستير في نظم المعلومات ، جامعة النيلين، 2016، ص13.
(2) مصباح عبد الهادي حسين الدويك، نظم المعلومات الصحية المحوسبة وأثرها على القرارات الإدارية والطبية، دراسة تطبيقية على مستشفى غزة الأوروبي ، رسالة ماجستير منشورة في الجامعة الإسلامية –غزة، 2010، ص 83.

وترجع أهمية السجل الطبيّ الإلكترونيّ إلى أنّه يتماثل مع السجل الطبيّ الورقي من حيث أوجه الاستعمال وأنّه قد يماثله – في نظر كثير من التشريعات– من حيث القوة القانونيّة المقررة له، بيد أنّ السجل الطبيّ الإلكترونيّ له كثير من المزايا التي تكفل له انتشاراً واسعاً وتزايداً مستمراً في الاستخدام.

لذلك، يعدّ السجل الطبيّ الإلكترونيّ تحولاً مهمّاً في القطاع الصحيّ، ليس لارتباطه بأفضل التقنيات والتجهيزات فائقة المستوى وحسب، وإنّما لشمولية فوائده وإيجابياته على صعيد التسهيلات الصحيّة التي توفرها السجلات الطبيّة المؤتمتة لجمهور المتعاملين، وامتداد ثمار الحوسبة لدعم اتخاذ القرار الطبيّ للأطباء والطواقم الطبيّة المساعدة والإداريين وتوحيد وتوثيق إجراءات العمل في المستشفيات والعيادات، وسرعة الوصول إلى البيانات الشاملة للمرضى في مواقع الرعاية الطبيّة[1].

وهكذا، فإنّ تطبيّق السجل الطبيّ الإلكترونيّ يحمل في طياته فوائد جمّة تنعكس إيجاباً على أداء مقدّمي الرعاية الصحيّة من جهة وعلى صحة المريض من جهة أخرى،فتطبيّق مثل هذه البرامج في المجالات الصحيّة يسهم في تقليل الأخطاء الطبيّة أقل بكثير من السّجلات الورقية، كما يحسّن التواصل بين الأطباء بشكل إيجابي مما يسمح لكل طرف بالوصول الكامل إلى التاريخ المرضي للشخص المعني.

**ثانياً: أهمية السجلات الطبيّة الرقميّة جنائيّاً**

لما كان السجل الطبيّ عبارة عن أرشيف حيوي يتطلب تسجيل جميع إجراءات الخدمة الصحيّة فيه،وهذا يعني أنه مع مشاكل الخدمة المختلفة في المستشفى يمكن أن يكون تنفيذ السجلات الطبيّة الرقميّة مع اللوائح الداخلية دليلاً أمام القضاء في حالة وجود وقائع وأخطاء طبيّة، فالحالة التاريخية لمتابعة حالة المريض الواردة في السجل هي دلالة واضحة على الإجراءات المتخذة قبله.

وتأسيساً على ما تقدم بيانه، نجد أنّ السجلات الطبيّة الرقميّة، هي أيضًا معلومات إلكترونيّة يقدمها مقدمو الرعاية بناءً على حالة المريض، التي يتم إرسالها إلى قسم آخر لمزيد من الاستشارة والفحص واستلامها وتخزينها في شكل رقميّ

(1) للمزيد انظر: السّجل الطبي الإلكتروني والسّجل الصحي الإلكتروني ما الفرق بينهما؟ وما هي الفوائد المرجوّة من تطبيقهما؟ موقع إلكتروني:https://www.thearabhospital.com

ويمكن عرضها في أي وقت إذا لزم الأمر،لذا بات قبول البيانات الرقميّة موضوع طبيّعي، وذلك لإقامة الدليل على وقوع الجريمة أمام القضاء ولتكوين القناعة الوجدانية للقاضي استناداً على الأدلة الرقميّة الجنائيّة[1]، ومن أجل منع الإجراءات التي تنتهك القانون، يوفر السجل الطبيّ الرقميّ أساسًا قانونيّاً فيما يتعلق بشرعية الأدلة الرقميّة والمتطلبات الإجرائية والموضوعية لقبولها كأدلة وقرائن رقميّة في ساحة القضاء.

فعند تفعيل السجلات الطبيّة لا بد من التأكد أنّه لدى رقمنة البيانات مثل السجلات الورقية لا توجد إمكانية لتعديلها حتى يمكن استخدامها كدليل أمام القضاء، بما في ذلك التوقيع الرقميّ، وتتمثل الجوانب الأساسية في تطبيّق نوعي السجلات الطبيّة سواء أكانت ورقية أم رقميّة في المصادقة والسرية، ويقصد بالمصادقة تحديد توقيع مستندات الملف الطبيّ في السجلات الورقية، بحيث يمكن لصق التوقيعات المباشرة على السجل الطبيّ للمريض، بينما في السجلات الطبيّة المؤتمتة، يمكن أن يكون التوقيع توقيعًا مؤتمتاً،بحيث تتضمن التوقيعات غير المعتمدة التوقيعات الممسوحة ضوئيًا؛ ويتم إدخال التوقيعات في الأجهزة الإلكترونيّة وبصمات الأصابع ومسح الشبكية أو كلمات المرور التي يمتلكها كل مستخدم لتحديد مصادقة صانع المستندات الإلكترونيّة. وكذلك، فإن التوقيع المعتمد هو توقيع رقميّ مع التشفير، وقد نصت على ذلك المادة (19) من قانون المعاملات الإلكترونيّة العماني، والمادة (15) من قانون المعاملات الإلكترونيّة الأردني رقم (15) لسنة 2015[2].

**المطلب الثاني: مظاهر التنظيم القانونيّ للسجل الطبيّ الرقميّ**

لمعالجة موضوع هذا المطلب، سنتناول في الفرع الأول: الالتزام بتنظيم السجلات الطبيّة الرقميّة، بينما نتناول في الفرع الثاني: حقوق المعني بمعالجة سجلاته الصحيّة الرقميّة.

(1) قضت محكمة بداية غرب عمان بقرار رقم 967 لسنة 2019، بأنه: "وبالرجوع لأحكام المواد (2،4،7) من قانون المعاملات الإلكترونية فإن المشرع أضفى على السجل الرقمي حجية الوثائق والمستندات الخطية في الإثبات خروجاً عن حكم القاعدة العامة التي لا تجيز للشخص أن ينشئ دليلاً لنفسه وذلك لاعتبارات أملتها الثقة والسرعة التي تتصف بها الأعمال التجارية، وحيث إنّ القيد الذي يتم تخزينه بوسائل رقمية يعتبر سجلاً مؤتمتاً بالمعنى المقصود في المادة (2) من قانون المعاملات الإلكترونية وأن لمخرجات الحاسوب قوة الإسناد العادية في الإثبات وفقاً لأحكام المادة (13/ج) من قانون البيانات وأن كشف الحساب التفصيلي موضوع الدعوى المسلسل رقم(3) من بيانات المدعية ينطبق عليه هذا الوصف ويعتبر قيداً إلكترونياً فإنه يتمتع بحجية الاسناد العادية للإثبات". منشورات مركز عدالة.

(2) المنشور في الجريدة الرسمية عدد (5341)، صفحة (5292)، تاريخ 2015/5/17.

**الفرع الأول: الالتزام بتنظيم السجلات الطبيّة الرقميّة**

أدى الاستخدام المتزايد للسجلات المحوسبة إلى تزايد في احتمالية تعرضها لخطر الانتهاك، من خلال الاعتداءات من قبل الموظفين الداخليين أو الأغراب، وقد تتسبب هذه الاعتداءات في أضرار مادية أو معنوية لكل من المستشفى والأفراد على حد سواء.

ويجب أن تفي سجلات المرضى المرقمنة التي يستخدمها مقدم الممارسة الطبيّة بمتطلبات إجراءات وقوانين الترخيص ذات الصلة، أو قد تواجه المنشآت الطبيّة عقوبات الترخيص،فالقوانين واللوائح التي تحكم ترخيص المستشفيات ومؤسسات الصيانة الصحيّة ومراكز العلاج ومقدمي الخدمات المؤسسية الأخرى بشكل عام تحتوي على معايير ومتطلبات محددة تتعلق بإنشاء سجلات المرضى والمصادقة عليها والاحتفاظ بها وتخزينها، فضلاً عن القيود المفروضة على وسائل الإعلام المسموح بإنشائها وتخزينها، والمتطلبات الإضافية الموجودة عادةً في قوانين ولوائح الترخيص الحكومية تتعلق بالسرية ومحتوى التسجيل والدقة والاكتمال والتوقيت وإمكانية الوصول.

وهكذا، تعدّ القضايا القانونيّة والتنظيمية من بين أكثر الجوانب صعوبة لدى تنفيذ الصحة المؤتمتة إذ يتعين معالجة الخصوصية والسرية، وحماية البيانات من أجل إنشاء بنى تحتية جديرة بالثقة[1]؛ كي يتم التمكن بالفعل من تطبيّق واستخدام مستدام لتطبيّقات الصحة الرقميّة. كما يمكن أنْ يؤدي الاتجاه المتزايد للمستشفيات إلى الاستفادة من الأنظمة الآلية للتكوين الطبيّ، مع عدم وجود قواعد ولوائح تشريعية محددة وواضحة إلى خروج المعلومات عن السيطرة ويزيد من احتمال تسرب المعلومات وإمكانية الوصول إليها من قبل سيء النية،وفي هذا تحدٍ جديد لمديري المعلومات الصحيّة وكذلك لمسؤولي المستشفيات فيما يتعلق بأدوارهم ومسؤولياتهم الجديدة.

لذلك، وضعت بعض البلدان قواعد محددة للسجلات الصحيّة الإلكترونيّة، بينما يعتمد بعضهم الآخر على تنظيم السجلات الصحيّة العامة بموجب قوانين حماية المعطيات والبيانات الذاتية. ويحلل هذا الفرع الإطار القانونيّ والتنظيمي للسجل الطبيّ المحوسب في أمريكا، وفي الاتحاد الأوروبيّ وأندونيسيا، على النحو التالي:

(1) أشرف عبد المحسن الشريف، أمن وحماية المستندات الإلكترونية على بوابة الحكومات العربية، مجلة علم، جامعة بني سويف، مصر، ع 16، يناير 2016 ، ص 83.

**أولاً: تنظيم السجلات الطبيّة الرقميّة في أمريكا**

لقد تطورت القواعد التنظيمية للبيانات التنظيمية الصحيّة المحمية خلال العقدين الماضيين، فكان الاهتمام بالسجلات الطبيّة الإلكترونيّة من جانب القطاع الخاص بداية، ولا سيما شركات التأمين ومؤسسات الرعاية الصحيّة، ولذلك، أصدرت الحكومة الأمريكية في عام 2009 أكبر حزمة تحفيز على الإطلاق من أجل تشجيع تبني حلول السجلات الطبيّة الرقميّة. ونظرًا للطبيّعة الحساسة للبيانات المخزنة في السجلات المؤتمتة، تم تقديم العديد من الضمانات من خلال قانون نقل التأمين الصحيّ والمساءلة (HIPAA)[1] وقانون تكنولوجيا المعلومات الصحيّة للصحة الاقتصادية والإكلينيكية (HITECH)، المدرجة في السجل الإلكترونيّ للصحة الخاصة بالمريض،حيث تم تناولها في قانون قابلية نقل التأمين الصحيّ.

وفي دراسة أُجريت على قانون التأمين الصحيّ لقابلية النقل والمساءلة (HIPAA) بعنوان قاعدة الخصوصية والصحة العامة، وبتوجيه من مركز السيطرة على الأمراض ووزارة الصحة والخدمات الإنسانية الأمريكية، أظهرت النتائج أنّ ضوابط ومعايير الخصوصية الجديدة للمعطيات الطبيّة والصادر عن قسم الخدمات الصحيّة والإنسانية بالولايات المتحدة (DHHS)، وفقًا لقانون القدرة على المنافذ والمساءلة للتأمين الصحيّ لعام 1996 (HI–PAA)[2]، لتوفير الحماية لخصوصية بعض المعطيات التي يمكن التعرف عليها بصورة ذاتية، والمشار إليها باسم البيانات الصحيّة المحمية (PHI) في محاولة للموازنة بين أمن المعطيات الصحيّة الذاتية للأفراد والحاجة إلى أمن الصحة العامة لأفراد المجتمع.

**ثانياً: تنظيم السجلات الطبيّة الرقميّة في الاتحاد الأوروبي**

تبنت الهيئات الحكومية في أوروبا تطوير السجلات الطبيّة المؤتمتة،فأنشأت عديد من الدول الأوروبية إطارًا قانونيّاً جديدًا بالتزامن مع بدء تطبيّق وتنفيذ هياكل الصحة الرقميّة التي أطلقتها الحكومات الأوروبية[3]. وفي عديد من

(1) The HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information: Final Rule") can be found at 45 Code of Federal Regulations (C.F.R.) parts 160 and 164. http://www.hhs.gov/ocr/AdminSimpRegText.pdf (accessed August 2, 2008). A summary of the HIPAA Privacy Rule, prepared by the HHS Office for Civil Rights, is available at http://www. hhs.gov/ocr/privacysummary.pdf (accessed october13, 2021)

(2) Fisher F, Madge B, Data security and patient confidentiality: the manager's role, International Journal of Biomedical Computing 1996; 43(1-2):115-9. doi: http://dx.doi.org/10.1016/S0020-7101(96)01236-6 .

(3)Stroetmann K., A.J., Stroetmann V.N. et al. European countries on their journey towards national eHealth infrastructures. 2011.

البلدان، يتم تنظيم استخدام الصحة الإلكترونيّة حاليًا –إن وجد– فقط من خلال الإطار القانونيّ العام، ولا سيما عن طريق القوانين المتعلقة بحقوق المرضى وحماية البيانات،من خلال التشريعات الحديثة.

ومن الجدير بالذكر أنّ توجيه الاتحاد الأوروبي في مارس 2011، المتعلق بحقوق المرضى في الرعاية الصحيّة عبر الحدود[1]، لم يهتم فقط باستحقاق وسداد خدمات الرعاية الصحيّة عبر الدول الأعضاء في الاتحاد الأوروبي، ولكن تم تناوله أيضًا لأول مرة صراحةً في المادة 14 من (European Health[2]) الفرص التي أتيحت من خلال أنظمة وخدمات قابليته للتشغيل البيني.

والتقدم الذي أحرزته الدول الأعضاء في إنشاء تشريعات تدعم خدمات الصحة الرقميّة، نظرًا لأنّ الجهود على المستوى الوطني لتنظيم الصحة الإلكترونيّة غالبًا ما تقتصر على مجالات محددة (مثل حقوق الوصول أو المسؤولية) ولا تغطي المواصفات الكاملة، فإنّ أي جهود مستقبلية للاتحاد الأوروبي لمواءمة التشريعات المتعلقة بالرعاية الصحيّة الرقميّة من أجل تقديم الرعاية الصحيّة عبر الحدود، تحتاج إلى الاعتراف بالتنوع الوطني والتطور هناك.

**ثالثاً: تنظيم السجلات الطبيّة الرقميّة في اندونيسيا**

تميزت دولة أندونيسيا بإصدار تشريعات صحيّة وخاصة الالتزام بعمل السجلات الطبيّة والمنصوص عليها في القانون رقم (29) لسنة 2004 وتعديلاته بشأن الممارسة الطبيّة[3]، فمع تقدم التقنيات بدأ الاعتماد على السجلات المؤتمتة بدل التقليدية، إلا أنّه لم يتم تنظيم التعليمات الفنية لاستخدام السجلات الطبيّة الإلكترونيّة في مختلف القوانين واللوائح، حيث تستخدم المستشفيات قانون ITE فقط كأساس لتطبيّق السجلات الطبيّة الرقميّة،ويتم تنظيم لائحة وزارة الصحة رقم 269 لعام 2008 بشأن السجلات الطبيّة سواء أكانت تقليدية أم إلكترونيّة، وهذا يعني أنّ اللائحة كشفت عن إمكانية تطبيّق السجلات الطبيّة المحوسبة بحكم القانون.

(1) European Union, Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare. 2011, Official Journal of the European Union: Brussels..
(2) Ibid.
(3) Moradi Gh. New dimensions of health-medical information and medical records management. Tehran: Vazhepardaz Publication; 2003.

وكذلك، فإن الالتزام بعمل السجلات الطبيّة منصوص عليه في منطوق المادة (46) من القانون رقم (29) لسنة 2004 بشأن الممارسة الطبيّة، وهو أنّ كلّ مستشفى ملزم بتنظيم السجلات الطبيّة، فيتعين أنْ تحتفظ مرافق الخدمات الصحيّة والممارسات الطبيّة بسجلات طبيّة.

نخلص إلى القول: إنّ بعض التشريعات تسمح صراحةً باستخدام السجلات الطبيّة المؤتمتة والمصادقة عليها والاحتفاظ بها، وتصرح تشريعات أخرى بمتطلبات السجلات الطبيّة للمستشفيات بشكل عام، وتسمح ضمنيًا بسجلات المرضى الإلكترونيّة، أو تتناول صراحة استخدام وظيفة واحدة فقط، مثل المصادقة، ولكن ليس لوظائف تسجيل المرضى.

**الفرع الثاني: حقوق المعني بمعالجة سجلاته الصحيّة الرقميّة**

**أولاً: حق إجراء تصحيّح السجلات الطبيّة في حالة وجود أخطاء في التسجيل**

تسمح بعض القوانين صراحةً للمريض أو لممثله المعتمد بفحص سجلات المستشفى الخاصة ببياناته الصحيّة ونسخها[1]، وقد لا تكون حقوق الوصول إلى السجلات الصحيّة التي يحتفظ بها الأطباء وغيرهم من مقدمي الرعاية الصحيّة الفردية واضحة دائمًا قبل أنْ تصبح السجلات متاحة، يجب على الشخص الذي يسعى للوصول عادةً أنْ يطلب هذا الوصول كتابيًا من المزود وقد يُمنح المرضى الحق في مراجعة سجلات المستشفيات الخاصة بهم فقط بعد الخروج من المشفى.

وتعدّ السجلات الطبيّة وثائق قانونيّة،ممّا يعني أنّه لا يمكن حذف المستند الطبيّ أو لا يمكن للمريض الوصول إليه،فإذا تم وضع لوائح لتصحيّح الأخطاء، فيجب الاحتفاظ بالوثائق الإلكترونيّة الأصلية (بما في ذلك الأخطاء) وإمكانية الوصول إليها، ومنع إساءة الاستخدام من قبل الأشخاص غير المصرح لهم[2]، ويعد أمن الشبكة المعلوماتية عنصراً أساسياً لمراقبة الوصول غير المصرح به إلى موارد هذه الشبكة،ففي هذه الحالة لا يمكن الوصول إلى البيانات إلا من قبل الجهات المصرح لها، حيث يمكن تحديد كل مستخدم بشكل متميز،وسيتم التعرف عليه بسهولة إذا ما قام مستخدم غير مصرح له بتغيير البيانات من خلال اسم مستخدم أو كلمة مرور.

(1) من نافلة القول إنّ المادة (11) من قانون حماية البيانات الشخصية العماني رقم (6) لسنة 2022 تنص على أنه": يكون لصاحب البيانات الشخصية الحق في الآتي:- أ-... ب- طلب تعديل بياناته الشخصية أو تحديثها أو حجبها...".

(2) إيهاب فوزي السقا، جريمة التزوير في المحررات الإلكترونية، دار الجامعة للنشر، الإسكندرية، 2002، ص14.

وما تجدر الإشارة إليه في هذا الشأن أنّ المقصود بخادم السجلات الطبيّة المحوسبة هو: أمين البيانات الصحيّة فهو المسؤول عن حفظ ومراقبة السجل الطبيّ للمرضى أو المؤسسات التي تُعد سجلات الرعاية الصحيّة وتحتفظ بها، ويجب أن يكون الوصي الرسمي مفوضًا بالتصديق على الملفات وإدارة جميع عمليات التفتيش أو نسخ السجلات، ويمكن استدعاؤه للإدلاء بشهادته على مقبولية السجل الرقميّ أمام الجهات المختصة.

**ثانياً: حق تخزين السجلات الطبيّة والتخلص منها**

لتخزين بيانات السجلات الطبيّة المؤتمتة يمكن للمستشفى وضع سياسة لتخزين المستندات الرقميّة بناءً على اللوائح الخاصة بها، ولأتلافها يمكن للمستشفى الرجوع إلى اللوائح المتعلقة بجدول الاحتفاظ بالسجلات داخل وزارة الصحة أو إتباع سياسة داخلية بشأن الإتلاف[1].

وتعد بيانات السجلات الطبيّة الإلكترونيّة ذات قيم مختلفة الاستخدامات، بما في ذلك الاستخدامات الإدارية أو البحثية أو القضائية، فقد سعى الباحثون (في علم الجينات مثلاً) وبشكل متزايد إلى البحث عن السجلات الطبيّة الرقميّة كمصدر غير مكلف لبيانات جينات الأفراد ، وبالتالي تحويل معلومات المرضى إلى مواضيع للبحث الجيني دون علمهم، ناهيك عن موافقتهم، في مناخ بحثي حيث يتم تجاهل مخاطر الخصوصية بشكل ممنهج ويمكن أنْ يكون أمن البيانات غير مؤكد.

**ثالثاً: حق إعطاء المصادقة على السجلات الطبيّة**

من المعلوم أنّ لكل سجل طبيّ اسماً وتوقيعاً ووقت وتاريخ للخدمات التي يؤديها أخصائي الرعاية، فالجوانب الأساسية في إدارة السجلات الطبيّة، سواء أكانت تقليدية أم مؤتمتة، هي المصادقة والسرية.

وتتحقق إجراءات التصديق من أنّ النسخة المقدمة هي نسخة طبق الأصل من النسخة الأصلية، ويمكن تقديم الشهادة باستخدام خطاب تصديق مكتوب يوضح أنّ النسخة المقدمة هي نسخة طبق الأصل من الأصل[2]، وتختلف

(1) مصباح عبد الهادي حسين الدويك ، نظم المعلومات الصحية المحوسبة وأثرها على القرارات الإدارية والطبية، دراسة تطبيقية على مستشفى غزة الأوروبي، رسالة ماجستير منشورة في الجامعة الإسلامية، فلسطين، غزة، 2010، ص 83. http://hdl.handle.net/20.500.12358/20011

(2)عبد الفتاح حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، ط1، دار النهضة العربية ، مصر، 2009، ص631.

القوانين في متطلبات الشهادة بشكل عام،فيكفي بيان وتوقيع أمين السجل في بعض القوانين، بينما تتطلب قوانين أخرى توقيع شاهد أو كاتب عدل أيضًا.

## المبحث الثاني: تأطير الحماية الجنائيّة للسجلات الطبيّة الرقميّة

لا ريب أنّمؤسسات الرعاية الصحيّة باتت تشهد ارتفاعًا ملحوظاً في انتهاكات البيانات والهجمات الإجرامية – مما عرض ملايين المرضى وسجلاتهم الطبيّة للخطر– ووفقًا لدراسة قام بها معهد بون يمون[1]، وهي دراسة معيارية حول خصوصية وأمن بيانات الرعاية الصحيّة فإنّ معظم مؤسسات الرعاية الصحيّة لا تزال غير مستعدة لمواجهة بيئة التهديد السيبرانيّ سريعة التغيير وتفتقر إلى الموارد والعمليات اللازمة لحماية بيانات المرضى، فالجناة يستهدفون قطاع الرعاية الصحيّة الغني بالبيانات؛ لأنّ المعطيات الذاتية للأفراد، والمعلومات الائتمانية، والبيانات الصحيّة يمكن الولوج إليها في مكان واحد –السجل الطبيّ– مما يُترجم إلى عائد مرتفع عند تحقيق الدخل وبيعه.

وفي ضوء ذلك تم تقسيم هذا المبحث لمطلبين: الأول لبيانالحماية الجنائيّة لسرية وخصوصية السجلات الطبيّة الرقميّة، والثاني لبيان بعص الجرائم الماسة برضا الشخص المعني بالمعطيات الطبيّة.

### المطلب الأول: الحماية الجنائيّة لسرية وخصوصية السجلات الطبيّة الرقميّة

لاشك أنّ الإشكالات الشائعة التي يتعين تناولها في البحث خلال المستندات الطبيّة المؤتمتة هي الخصوصية والسرية[2]، وتعدّ الواجبات القانونيّة للحفاظ على السرية وتجريم الولوج إلى كل ما يتعلق بالسجلات الورقية والرقميّة. ومع ذلك، فإنّ الاحتفاظ بسرية وخصوصية السجلات الرقميّة من الوصول غير المسموح بها يعد تحدياً، ويمكن أنْ يكون للفشل في القيام بذلك عواقب وخيمة أكثر مما قد يحدث في حالة السجلات التقليدية. من هنا تم تخصيص الفرع الأول للحماية الجنائيّة لسرية السجلات الطبيّة الرقميّة، والفرع الثاني للحماية الجنائيّة لخصوصية السجلات الطبيّة الرقميّة.

(1) Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data. https://lpa.idexpertscorp.com/acton/attachment.

(2) تنص المادة (44) من قانون المعاملات الإلكترونية العماني رقم (69) لسنة 2008 على أنه: "يتعين على مقدم خدمات التصديق اتباع الإجراءات المناسبة لضمان سرية البيانات الشخصية التي في عهدته في سياق القيام بواجباته ولا يجوز له إفشاء أو تحويل أو إعلان أو نشر تلك البيانات لأي غرض مهما كان إلا بموافقة مسبقة من الشخص الذي جمعت عنه البيانات".

**الفرع الأول:الحماية الجنائيّة لسرية السجلات الطبيّة الرقميّة**

هناك دائمًا تحديات تتعلق بالسرية وخاصة نوع الإفصاح والإفراج عنها في أقسام السجلات الطبيّة الرقميّة، والسرية تفرض في موضوع الرعاية الصحيّة التزام المهنيين الذين لديهم فرصة في الولوج للسجلات أو اتصالاتهم بحفظ سرية البيانات المحوسبة، ويمكن تعريف السرية أيضاً على أنّها حصر البيانات الذاتية على الأفراد غير المسموح لهم بالولوج إلى البيانات أثناء التخزين أو الإرسال أو عند معالجتها، وهذا ما أورده قانون الجزاء العماني رقم 7 لسنة 2018 في نص المادة (331) منه.

ويمكن توفير سرية المستندات الطبيّة عبر الطرق التقنية مثل تشفير البيانات أو من خلال التحكم في الوصول إلى الأنظمة، وتتحقق السرية أيضًا من خلال العمل على السلوكيات الأخلاقية مثل الصمت المهني، وتعد السرية في الرعاية الصحيّة متجذرة في سرية العلاقة بين المريض والمؤسسة الصحيّة،وهذا المفهوم أساس لإرشادات المهنيين الطبيّين للسرية، إنّ الالتزام بالحفاظ على سرية البيانات الطبيّة مدعوم في قواعد أخلاقيات الجمعيات المهنية،وقد نصت المادة (16) من (قانون رقم 2 لسنة 2019) الإماراتي بشأن تقنية المعلومات والاتصالات في المجالات الصحيّة على أنه[1]: "...: أ. تداول المعلومات الضرورية لإنجاز العمل المطلوب أو الغرض المحدد. ب. أنْ يقتصر تداول المعلومات مع الأشخاص المصرح لهم دون غيرهم. جـ. عدم تعديل البيانات والمعلومات الصحيّة بالحذف أو بالإضافة إلا وفقاً للضوابط المحددة. د. عدم نشر البيانات والمعلومات الصحيّة وكذلك الإحصائيات المتعلقة بالمجال الصحيّ إلا وفقاً للضوابط المحددة".

وعليه، نجد أنّ نص المادة (16) من ذات التشريع قد تضمنت مواضيع سرية المعطيات الخاصة بحالة المرضى والاستثناء منها، فيتعين على كل من يتداول المعلومات الخاصة بالمرضى المحافظة على سريتها وعدم استخدامها لغير الأغراض الصحيّة دون موافقة خطية من المريض، باستثناء البيانات التي تقدم لشركات التأمين على الحياة أو المؤسسة

(1) تنص المادة (20) من قانون رقم 2 لسنة 2019 بشأن تقنية المعلومات والاتصالات في المجالات الصحية الإماراتي على أنه: "1. يشترط في حفظ البيانات والمعلومات الصحية بواسطة تقنية المعلومات والاتصالات ما يأتي: أ. أن تتناسب مدة الحفظ مع الحاجة إلى البيانات والمعلومات الصحية، على ألا تقل مدة الحفظ عن (25) خمس وعشرين سنة من تاريخ آخر إجراء صحي للشخص المعني بتلك البيانات والمعلومات الصحية. ب. ضمان معايير السرية وصحة ومصداقية البيانات والمعلومات. 2. تحدد اللائحة التنفيذية لهذا القانون ضوابط وإجراءات تنفيذ أحكام هذه المادة".

الصحيّة، وأغراض البحث والسريري، ويهدف اتخاذ الإجراءات الوقائية والعلاجية المتعلقة بالصحة العامة، وبناء على طلب الجهات المختصة، واستجابة لإجراءات الجهة الصحيّة لأغراض الرقابة والتفتيش.

وكذلك، نجد في المبدأ الأول من مدونة أخلاقيات إدارة البيانات الصحيّة الأمريكية[1] "الدفاع عن حق الفرد في الخصوصية والعقيدة، والتمسك به، والدفاع عن السرية في استخدام المعلومات والكشف عنها، ويعرف القانون السرية على أنّها اتصال متميز بين طرفين في علاقة مهنية، مثل التواصل مع المريض والطبيب أو الممرضة أو غيره من المهنيين الطبيّين في حين إنّ التطبيّق في الإجراءات القانونيّة يخضع لقواعد الإثبات ومراعاة الحاجة العامة للمعلومات، ومن التطبيّقات على ذلك الحكم في قضية (Jaffee v. Redmond) حيث أيدت المحكمة العليا الأمريكية، رفض المعالج الكشف عن معلومات العميل الحساسة أثناء المحاكمة[2] .

وعند النظر في البيانات الطبيّة الحساسة[3] فالبيانات والمعطيات الحساسة تتطلب درجات خاصة من السرية، مثل علاج الصحة العقلية، ففي ولاية إلينوي الأمريكية مثلاً، يقدم قانون خصوصية الصحة العقلية والإعاقات[4] إجراءات مفصلة للدخول إلى بيانات المريض السرية واستخدامها والكشف عنها بما في ذلك الإجراءات القانونيّة.

وما تجدر الإشارة إليه، أنّه في إنجلترا يجب الاحتفاظ بالبيانات الصحيّة باعتبارها سراً طبيّاً، ويحق للمريض فقط الاطلاع على محتويات السجل الطبيّ، ومن اللوائح التي تلزم حفظ الأسرار الطبيّة هي اللائحة الحكومية رقم 10 لعام 1966 المتعلقة بالحفاظ الإلزامي للأسرار الطبيّة في المادتين (1 و 2)[5]، التي تم تعديلها من خلال لائحة وزارة الصحة رقم 36 لعام 2012 المتعلقة بالأسرار الطبيّة، بشكل عام تنظيم الالتزام والاحتفاظ ببيانات السجلات الصحيّة السرية واردة ومنظمة بصورة صريحة في لوائح وزارة الصحة.

(1) AHIMA. (2011). American Health Information Management Association Code of Ethics. http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_024277.hcsp?dDocName=bok1_024277

(2) Beyer, Karen. (2000). "First Person: *Jaffee v. Redmond* Therapist Speaks." *American Psychoanalyst*, Volume 34, no. 3. Retrieved from http://jaffee-redmond.org/articles/beyer.htm

(3) عرفها قانون حماية البيانات المصري رقم(151) لسنة 2020 في المادة (1/ج) منه على أنها: ( البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية، أو بيانات القياسات الحيوية "البيو مترية" ...).

(4)Mental Health and Developmental Disabilities Confidentiality Act (MHDDCA) (740 ILCS 110). Effective July 1, 1997. Illinois General Assembly. Retrieved from http://www.ilga.gov/legislation

(5) Legislation covering medicines. https://www.health-ni.gov.uk/articles/legislation-covering-medicines#toc-11.

أمّا في التشريع الأردني فلم ترد نصوص مباشرة وصريحة تعالج انتهاك البيانات والمعلومات الطبيّة والصحيّة الرقميّة، وإنّما اقتصرت على الإشارة إلى الاعتداء على الرسائل الإلكترونيّة في المادة (5) من قانون الجرائم الإلكترونيّة رقم (27) لسنة 2015[1]، وجرائم الذم والقدح والتحقير الإلكترونيّة (نشر أو إرسال أو إعادة إرسال بيانات أو معلومات عن طريق الشبكة المعلوماتية أو الموقع الإلكترونيّ أو نظام معلومات) في المادة (11) من القانون ذاته، وخرق حرمة الحياة الخاصة في المادة (348 مكررة) من قانون العقوبات رقم (16) لسنة 1960[2]، وإفشاء الأسرار التي حصل عليها الشخص بحكم وظيفته أو مهنته في المادة (355) من القانون ذاته.

وأضف إلى ذلك أنّ المادة (8/هـ) من قانون المسؤولية الطبيّة والصحيّة الأردني رقم (25) لسنة 2018[3] اكتفت بمنع مقدم الخدمة من إفشاء أسرار متلقي الخدمة التي اطلع عليها أثناء مزاولة المهنة أو بسببها، مما يشكل قصوراً تشريعياً في مساءلة من يقوم بنشر وتداول البيانات والمعلومات الطبيّة والصحيّة جنائيّاً.

ولذا نتمنى على المُشَرِّع الأردني فرض السرية على البيانات والمعلومات الطبيّة والصحيّة الرقميّة، وذلك بتجريم إفشائها بنص صريح، وتقرير المسؤولية الجنائيّة لناشري ومتداولي هذه البيانات والمعلومات.

**الفرع الثاني:الحماية الجنائيّة لخصوصية السجلات الطبيّة الرقميّة**

بادئ ذي بدء، تعرف الخصوصية الرقميّة بأنّها[4]: (حق الفرد في أنْ يضبط عملية جمع البيانات الشخصية، ومعالجتها آلياً، وحفظها، وتوزيعها، واستخدامها في صنع القرار الخاص به أو المؤثر فيه).

وفي هذا السياق، يعدّ الأمن السيبرانيّ وثيق الصلة كما هو الحال في عمليات وممارسات المستشفى، ولكن مخاطر الخصوصية التي تنجم عن الكشف عن البيانات الطبيّة والجينية تؤدي دورًا بارزًا، وأضحت تشكل عائقاً أمام تقدم العلوم الطبيّة ممّا انعكس على تطور التشريعات واللوائح الصحيّة بحيث أضحت أكثر صرامة ومنها على سبيل المثال

(1) المنشور في الجريدة الرسمية عدد (5343)، صفحة (5631)، تاريخ 2015/6/1.
(2) المنشور في الجريدة الرسمية عدد (1487)، صفحة (374)، تاريخ 1960/5/11.
(3) المنشور في الجريدة الرسمية عدد (5517)، صفحة (3420)، تاريخ 2018/5/31.
(4) د. محمد المقاطع، حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسوب الآلي، الكويت (د.ن)، 1992، ص45.

HIPAA في أمريكا والقانون العام لحماية البيانات في الاتحاد الأوروبي[1]، بخلاف التشريع الأردني الذي لم يوفر حماية مباشرة للمعلومات والبيانات الطبيّة والصحيّة، ولم ينظم تبادل هذه المعلومات والبيانات وجمعها وتخزينها وتسجيلها وحفظها واستعمالها وتوزيعها وإتلافها وغيرها من الإجراءات.

وهكذا، تشير الخصوصية إلى الحق الذي يجب على شخص ما أنْ يقرر بنفسه متى وكيف ومستوى نقل المعلومات الشخصية أو مشاركتها من قبل الآخرين[2]، ويُنظر إلى الخصوصية على أنها حق العميل أو المريض في التخلي عنها، واتخاذ قرارات بشأن كيفية مشاركة المعلومات الشخصية، فعندما يدرك المرضى ومقدمو الخدمة أن السجلات المستندة إلى الرقمنة تزيد من تهديد خصوصية المريض، فقد لا يرغبون في تقديم أو تسجيل معلومات كاملة في سجل المريض، لا سيما الحالات المتعلقة بالمسائل الحساسة، مثل عمليات الإجهاض، والإيدز، والمشاكل النفسية، وتعاطي المخدرات أو الكحول...الخ.

لذلك، فإنّ الافتقار إلى الحماية القانونيّة الملائمة لخصوصية المرضى خاصة ما يتعلق بسجلات المرضى قد يكون عائقاً أمام تطور أنظمة سجلات المرضى المعتمدة على الشبكة المعلوماتية،ويمكن انتهاك الخصوصية في عديد من المواقف من خلال تحديد منهجي لا يمكن منعه الذي يحدث في أنظمة السجلات الطبيّة، ومن خلال التكنولوجيات المركزية والأطراف التي تنظر في تصرفات العاملين في مجال الرعاية الصحيّة والمرضى فعلى الرغم من أنّ الدستور الأمريكي مثلاً لا يحدد "الحق في الخصوصية"، فقد تم تحديد حقوق الخصوصية فيما يتعلق بإجراءات الرعاية الصحيّة والمعلومات الطبيّة في قرارات المحاكم، وفي القوانين الفيدرالية وقوانين الولايات، وإرشادات المنظمة المعتمدة ومدونات الأخلاق المهنية.

ويعد التطبيّق الأهم لحماية الخصوصية للمرضى قاعدة الخصوصية الفيدرالية[3] HIPAA، التي تصدر معايير لضمان خصوصية المعطيات الطبيّة ولتحديد "البيانات الصحيّة المحمية، والهدف من قاعدة خصوصية HIPAA هو تحديد وتقييد الظروف التي يمكن فيها تبني البيانات الطبيّة الآمنة للفرد أو الكشف عنها،فقدتم إنشاؤه وفقًا لقانون إخضاع

(1) Regulation 2016/679 of the European parliament and the Council of the European Union. Brussels: Off J Eur Communities; 2016: 1–88.

(2) بولبين أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، منشورات الحلبي الحقوقية، بيروت، 2009، ص56.

(3) U.S. Department of Health and Human Services (HHSa), Office for Civil Rights. (2003). Summary of the HIPAA Privacy Rule. Retrieved from: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

التأمين الصحيّ لقابلية النقل والمساءلة لعام 1996 (HIPAA) ، كما هو موضح من جانب وزارة الصحة والخدمات الإنسانية الأمريكية (HHS)، وقاعدة الخصوصية، حيث تحقق توازنًا يسمح باستخدامات مهمة للمعلومات، مع حماية خصوصية الأفراد الذين يسعون للحصول على الرعاية والشفاء، ويتم تزويد الأفراد ببعض عناصر التحكم، مثل الحق في الولوج إلى البيانات الصحيّة المتعلقة بهم في معظم الأحيان، والحق في طلب تعديل البيانات الصحيّة المشكوك بها، فهذه محاولة لتحقيق التوازن،فالقاعدة توفر استثناءات عديدة لاستخدام الكشف عن البيانات المحمية دون رضا المريض، بما في ذلك العلاج، والأنشطة الصحيّة المختلفة.

وحتى قبل أنْ تهيمن HIPAA على خصوصية الرعاية الصحيّة،فهناك حكم مهم للمحكمة العليا بأمريكا في قضية(Whalen v. Roe) [1]، وهذا الحكم متعلق بالحق في خصوصية المعلومات الصحيّة، حيث اعتبرت هذه القضية قانونًا أساسيًا لولاية نيويورك يتطلب من الأطباء تقديم تقرير للدخول إلى قاعدة البيانات المحوسبة لإدارة الصحة في نيويورك حول وصف أنواع معينة من الأدوية التي يُحتمل إساءة استخدامها أو وصفها بشكل مفرط؛ وقد تضمنت المعلومات اسم المريض والطبيب والصيدلية وجرعة الدواء،حيث رفعت مجموعة من المرضى واثنتان من جمعيات الأطباء دعوى قضائية، مدعية أنّ هذا الإجراء ينتهك العلاقة المحمية بين الطبيب والمريض وقد أقرت المحكمة بمصلحة الفرد في حماية خصوصيته مع إعطاء وزن أكبر لحق الدولة في معالجة قضية تهم المجتمع،حيث تناول حكم المحكمة العليا في قضية Whalen v. Roe مبدأ الاهتمام المتوازن في قاعدة الخصوصية اللاحقة. بقولها "... إن الإفصاح عن المعلومات الطبيّة الخاصة للأطباء وموظفي المستشفيات وشركات التأمين ووكالات الصحة العامة غالبًا ما يكون جزءًا أساسيًا من الممارسات الطبيّة الحديثة"، لم تمنح المحكمة الأفراد سيطرة مطلقة على معلوماتهم الصحيّة، ومن المثير للاهتمام، أنّ قرار Whalen أشار أيضًا إلى الاهتمام المتزايد بجمع البيانات الخاصة في صورة رقميّة.

**المطلب الثاني:الجرائم الماسة برضا الشخص المعني بالمعطيات الطبيّة**

سنتناول في هذا المطلب صور لبعض الجرائم الماسة برضا الشخص المعني بالمعطيات الطبيّة، وذلك في فرعين، حيث سنخصص الفرع الأول لجريمة معالجة المعطيات الشخصية دون رضا المريض، والفرع الثاني لجريمة المساس بحقوق الشخص المعني بالمعطيات الطبيّة.

(1) Whalen v. Roe, 429 U.S. 589 (1977), https://supreme.justia.com/cases/federal/us/429/589/.

**الفرع الأول: جريمة معالجة المعطيات الشخصية دون رضا المريض**

تنص المادة (5) من قانون حماية البيانات الشخصية العماني رقم 6 لسنة 2022 على أنّه "تحظر معالجة البيانات الشخصية التي تتعلق بالبيانات الجينية أو البيانات الحيوية أو البيانات الصحيّة...إلا بعد الحصول على تصريح بذلك..."، وتنص المادة (28) من القانون ذاته على أنّه "يعاقب بغرامة لا تقل عن (15000) خمسة عشر ألف ريال عماني ، ولا تزيد على (20000) عشرين ألف ريال عماني، كل من يخالف أحكام المواد(5) ...".

يلاحظ بأن البيانات الطبيّة تمتاز بالسرية التامة، حيث إنّ الملف الإلكترونيّ للمريض لا يطلع عليه أحد سوى المريض، والممارس الصحيّ المخول من لدن إدارة المؤسسة الصحيّة أو الإدارة حسب الاختصاص، ويتم إتباع السياسات والإجراءات المحلية والدولية لتلافي أي أضرار على المرضى، حيث تطبق معايير السلامة للمرضى ومن أمثلتها طلب وصرف الأدوية للمريض.

ونجد كذلك بأنه وبموجب القانون الفيدرالي الكندي[1]، يمتلك المريض البيانات الواردة في السجل الطبيّ، لكن مقدم الرعاية الصحيّة يمتلك السجلات بنفسه، وعندما يكون المزود موظفًا في عيادة أو مستشفى، فإن صاحب العمل هو صاحب السجلات، بموجب القانون، يجب على جميع مقدمي الخدمة الاحتفاظ بالسجلات الطبيّة لمدة 15 عامًا بعد الإدخال الأخير.

ومن التطبيّقات القضائية المهمة للمحكمة العليا الكندية لعام 1992 في قضية ماكنيرني ضد ماكدونالد[2]، (McInerney *v.* MacDonald) حيث تم رفض استئناف قدمته الطبيبة إليزابيث ماكينيرني، للطعن في حق وصول المريض إلى سجله الطبيّ، تمكنت المريضة مارجريت ماكدونالد بأمر من المحكمة من حق الوصول إلى سجلها الطبيّ الخاص، وقد واجهت القضية معضلة قانونيّة لكون السجلات الطبيّة للمريضة كانت في شكل إلكترونيّ، وتحتوي على معلومات وبيانات قدمها مقدمو خدمات آخرون، وقد أكدت ماكنيرني أنها لا تملك الحق في إصدار السجلات الطبيّة التي لم تقم بإصدارها بنفسها، فالتشريع الكندي يعتبر مقدمي الخدمة الرقميّة مالكين للسجلات الطبيّة الصحيّة، بيد أنّه منح المريض حق الوصول إلى السجلات الطبيّة بنفسه.

(1) Medical record.Wikipediasite:emirate.wiki
(2) McInerney *v.* MacDonald, [1992] 2 S.C.R. 138.
https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/884/index.do

وتقدم برامج السجلات الصحيّة الإلكترونيّة هدفًا مغريًا للجناة، فمنذ أنْ أصدر الكونجرس الأمريكي قانون قابلية التأمين الصحيّ والمساءلة (HIPAA) في عام 1996 يتعين على الهيئات التي لديها سجل صحيّ إلكترونيّ حماية معلومات المريض الحساسة من مجرمي الكمبيوتر العازمين على اقتحام النظام.

وبخلاف ذلك، يتم توجيه دعاوى قضائية من المرضى إذا تم اختراق معلوماتهم، وهناك خطر آخر يجب أخذه في عين الاعتبار وهو احتمال اختطاف السجلات الإلكترونيّة بواسطة فيروسات "الفدية" تحتجز بيانات المريض كرهينة، ويتم تشفيرها حتى تدفع رسوم برنامج الفدية لإلغاء تأمين المعلومات.

وقد يؤدي الكشف الجماعي عن معلومات المريض إلى مسؤولية كارثية لمقدم الخدمة؛ يمكن أنْ يؤدي أيضًا إلى عقوبات الترخيص أو عقوبات جزائية، تشمل القواعد التي يمكن بموجبها تحميل مقدمي الخدمة مسؤولية انتهاك مبدأ السرية استناداً للقانون العام، وتشمل قواعد القانون العام التي يمكن بموجبها تحميل مقدمي الخدمة المسؤولية عن انتهاكات السرية والخصوصية، وخيانة الأسرار المهنية، والافتراء، والإهمال.

**الفرع الثاني: جريمة المساس بحقوق الشخص المعني بالمعطيات الطبيّة**

جاء في نص المادة (5) من قانون مكافحة جرائم تقنية المعلومات العماني رقم (12) لسنة 2011 أنّه: "يعاقب بالسجن ...، كل من غيّر أو عدّل أو أتلف عمداً دون وجه حق باستخدام وسائل تقنية المعلومات بيانات أو معلومات إلكترونيّة عبارة عن تقرير فحص أو تشخيص أو علاج أو رعاية طبيّة مخزن في نظام معلوماتي أو وسائل تقنية المعلومات". وذلك بخلاف قانون الجرائم الإلكترونيّة الأردني رقم (27) لسنة 2015 الذي خلت نصوصه من توفير حماية جنائيّة مباشرة للبيانات الشخصية بما في ذلك البيانات الطبيّة والصحيّة، من الاعتداء عليها بالنسخ أو النقل أو التغيير أو التعديل أو الإضافة أو الحذف أو الإتلاف وغيرها من صور الاعتداء.

وفي إطار تطوير القطاع الصحيّ والخدمات الصحيّة الفرنسي، أورد المرسوم رقم 960-2007 بتاريخ 15 أيار 2007 تدابير ومعايير سرية البيانات المخزنة حاسوبياً أو المنقولة عبر الطرق الإلكترونيّة[1]. ونص قانون المعلوماتية والحريات الفرنسي الصادر بتاريخ 6 يناير 1978 المعدل بموجب قانون 20 يونيو 2018 في مادته 38 و 39 على حق الدخول إلى المعطيات الطبيّة الذاتية وحق اعتراض المعني على تبادل المعلومات الخاصة به لأسباب قانونيّة، ونصت المادة 1110-4 بند 3 من قانون الصحة العامة الفرنسي الصادر في عام 1953، والمعدل بموجب مرسوم عام 2000 و 2003 و 2005[2]، على أنّ: "المريض الموجود بعناية الفريق الطبيّ في مؤسسة صحيّة، تكون المعلومات التي تعنيه، وبإرادته بعهدة مجموع الفريق، وكذلك إذا تعلق الأمر بمجموعة معالجين في عيادة و مركز طبيّ...". ويبقى رضا المريض مطلوباً قانوناً وبشكل صريح عند تخزين المعلومات واستضافتها بحسب نص المادة 1111-8 بند 2 من قانون الصحة العامة الفرنسي.

ويمكن ملاحظة الالتزامات القانونيّة فيما يتعلق بخصوصية وأمن البيانات بصورة غير مباشر في أحكام المواد (30 إلى 33 والمادة 35) من قانون ITE رقم 19 لعام 2016 الإندونيسي[3]، الذي ينظم الأعمال المجرمة، في هذه الحالة، يجرم قانون ITE أي شخص استخدام الأنظمة الإلكترونيّة للولوج للنظام بصورة غير مصرح بها، مما يتسبب في اتخاذ إجراءات غير قانونيّة ضد بيانات الآخرين للحصول على معلومات عن طريق التلاعب بها أو تبديلها أو إزالتها عن طريق الولوج غير المشروع إلى أمن الأنظمة الرقميّة في السجلات الطبيّة المؤتمتة من خلال أولئك الذين يتمتعون بالسلطة، هم مقدمو الخدمات الطبيّة، بما في ذلك الأطباء والصيادلة وأخصائي التغذية والمسعفون،وتتضمن المعطيات في السجلات بيانات ومعطيات المريض الاجتماعية والمرضية...إلخ.

لذلك، يمكن إساءة استخدامها بما في ذلك التشخيص ومعلومات العلاج، ومن هذه المعلومات هناك احتياجات خاصة من الهيئات المختلفة، بما في ذلك خدمات الصحة العامة والشركات، على سبيل المثال، شركات التأمين والمحاكم

(1)Décret n°2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique (dispositions réglementaires). **https://www.wpirg.org/wp-co.**

(2) Code de la santé publique. Dernièremise à jour des données de cecode : 09 octobre 2021.
(3) Law No. 19 of 2016 on the Amendment to Law No. 11 of 2008 on Electronic Information and Transactions. https://www.humanrightspapua.org/resources/nlaw/734-law-no-19-of-2016-on-the-amendment-to-law-no-11-of-2008-on-electronic-information-and-transactions

إذا كان هناك أمر للحصول على البيانات، وفقًا للوائح، فإن الإفراج عن السجلات الطبيّة من المستشفى يعتمد فقط على أوامر أو طلبات المحكمة، لذلك فمن الضروري الاستمرار في معالجة قضايا مثل الوصول إلى المعلومات وتحديثها في سجلات السجلات الطبيّة الإلكترونيّة.

## الخاتمة

غالبًا ما تعني قدرة أنظمة المعلوماتية على جمع كميات من المعلومات وتخزينها والسماح بالوصول إليها، لذلك يتم جمع المزيد من المعلومات وتخزينها على أنظمة تسجيل قائمة على الكمبيوتر أكثر مما يتم جمعه وتخزينه في السجلات الورقية، نظرًا لقدرة الكمبيوتر على التخزين والنسخ، ويمكن أنْ يؤدي خرق واحد لأمن النظام إلى الكشف غير المصرح به عن معلومات شاملة حول أعداد كبيرة من المرضى.

وأضف إلى ذلك، فإنّ قدرة الكمبيوتر على تقديم المعلومات لأعداد كبيرة من المرضى في وقت واحد تجعل أنظمة تسجيل المرضى المعتمدة على الكمبيوتر هدفًا أكثر إغراءً من السجلات الورقية؛ لأنّ البيانات المدرجة في سجلات المرضى تصبح أكثر تعقيدًا مثل المعلومات الجينية.

وهكذا، فإنّ مناقشة موجزة للقضايا القانونيّة الرئيسية التي تثيرها سجلات المرضى وأنظمة السجلات المستندة إلى الكمبيوتر: القضايا التنظيمية والاعتماد، وقضايا الأدلة، وخصوصية المريض ومخاوف الوصول إلى السجلات، وأسئلة ملكية السجل.

وتبقى السجلات الطبيّة المحوسبة الميزة الأهم والأفضل للتطورات في عالم السجلات الطبيّة، ومن أكبر تحديات هذا التطور الطبيّ متابعة كميات هائلة من المعلومات الطبيّة المتعلقة بالمرضى وحمايتها من أي خروقات أو انتهاكات.

## النتائج:

1- لا تزال هناك بعض القوانين والأنظمة المعنية بترخيص المستشفيات تفرض تحديات تحول دون التفعيل الآلي الكامل لسجل المريض الإلكترونيّ، وهناك فرق بين دولة وأخرى في متطلبات السجلات الطبيّة والقوانين واللوائح القديمة أو المتضاربة وهنالك عقبات أمام التطوير الكامل لأنظمة سجلات المرضى المعتمدة على الحوسبة.

2- عدم تنظيم اللوائح والأنظمة المتعلقة بالتعليمات الفنية لإدارة السجلات الطبيّة باستخدام التكنولوجيا الرقميّة، إنّ اعتماد مثل هذه التقنيات في مجال حسّاس كالمجال الصحيّ يقتضي وضع قواعد دقيقة تضمن الحفاظ على حقوق كل طرف وتحديد واجباته، وهذه القواعد تهم خاصية سلامة وأمن البيانات والمعلومات الصحيّة، وكيفية تبادلها، وضمان سرّيّتها وحمايتها وموثوقيتها، تحقيقاً لاستخدامها بصفة سليمة وآمنة.

3- السجل الطبيّ الإلكترونيّ الفعلي يمكن استخدامه كدليل أصيل في المحكمة في حالة حدوث نزاع طبيّ. لذلك، يهتم المختصون بفحص وضع السجلات الطبيّة الإلكترونيّة كدليل في المحكمة.

4- يمثل الربط الإلكترونيّ والملف الموحد الخاص بكل مريض في الدولة إنجازاً وتطوراً فريداً في مسار تقديم مقومات الرعاية الصحيّة التي تفوق توقعات الأفراد وفق أعلى الممارسات العالمية في جودتها واستدامتها نحو استشراف المستقبل، في إطار استراتيجية تقديم الرعاية الصحيّة بصورة متكاملة، وتطوير نظم البيانات الصحيّة،وإنشاء أنظمة الجودة والسلامة الطبيّة، وترسيخ ثقافة الابتكار.

5- تستخدم ثلاثة مفاهيم مهمة وذات صلة بالتبادل في مناقشة حماية البيانات الصحيّة داخل نظام الرعاية الصحيّة: السرية والخصوصية والحماية ومع ذلك، فإنّ كلّ من هذه المفاهيم لها معنى أساس مختلف ودور فريد. من أجل حماية سرية السجلات الصحيّة ومنح المرضى حقوق الوصول إلى سجلاتهم الصحيّة والحق في تضمين تصحيّحات للمعلومات في السجلات الصحيّة.

**المقترحات:**

**أولاً:** أن يقوم المُشَرِّعان الأردني والعُماني بتنظيم تبادل معلومات وبيانات المرضى الرقميّة وجمعها وتخزينها وتسجيلها وحفظها واستعمالها، وأي إجراء آخر يتم عليها،كونها من الأمور الشخصية التي لا تعد ملكاً للجهة الصحيّة،التي تمنع أخلاقيات مهنة الطب الإفشاء عنها أو إعطاءها لأي شخص، وذلك بوضع الضوابط اللازمة لضمان اعتماد المستندات والاتصالات في أفضل الظروف، والاستفادة منها بأقصى قدر ممكن لتوفير الخدمات الصحيّة المناسبة للمريض، وتيسير التواصل بين كل المتعاملين والمتدخلين في الشأن الصحيّ.

**ثانياً:** أنْ يقوم المُشَرِّعان العماني والأردني بفرض السرية على البيانات والمعلومات الطبيّة الرقميّة، وذلك بتجريم إفشائها بنص صريح، وتقرير المسؤولية الجنائيّة لناشري ومتداولي هذه البيانات والمعلومات.

**ثالثاً:** ضرورة قيام المُشَرِّع الأردني بحماية حقوق الشخص المعني بالمعطيات الطبيّة، وذلك بتجريم كافة أشكال وصور الاعتداء على البيانات والمعلومات الطبيّة كالنسخ والنقل والتغيير والتعديل والإضافة والحذف والإتلاف وغيرها من صور الاعتداء

**رابعاً:** إنشاء قاعدة بيانات صحيّة تشاركية على مستوى الدولة، لزيادة مستويات الرعاية الصحيّة، وتعزيز مشاركة المرضى، والمحافظة على خصوصيتهم، وفق أعلى المعايير العالمية، إذ ستؤدي الصحة الرقميّة دوراً رئيساً في مستقبل الخدمات الصحيّة.

# المصادر والمراجع

## المراجع باللغة العربية:

- إيهاب فوزي السقا، جريمة التزوير في المحررات الإلكترونيّة، دار الجامعة للنشر، الإسكندرية، 2002 .
- عبد الحميد بسيوني، الصحة الإلكترونيّة، الطبعة الأولى، دار الكتب العلمية للنشر والتوزيع، القاهرة، 2008.
- عبد الفتاح حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، ط1، دار النهضة العربية، مصر، 2009.
- فايز النجار، نظم المعلومات الإداريّة، دار الحامد للنشر والتوزيع، عمان، 2007.
- لمياء الخليفة، بناء نظام السجلات الطبيّة، بحث تكميلي لنيل درجة الماجستير في نظم المعلومات، جامعة النيلين، 2016.
- مصباح عبد الهادي حسين الدويك، نظم المعلومات الصحيّة المحوسبة وأثرها على القرارات الإدارية والطبيّة: دراسة تطبيّقية على مستشفى غزة الأوروبي، رسالة ماجستير منشورة في الجامعة الإسلامية – غزة، 2010.

## المراجع العربية (المرومنة):

-Āīhabalsqā, jrīmh AL-tazwirfī Al-muharrat AL-ktrūnyā, dāraljam‘h, Al-Āskandrīh, 2002.

-‘bd, Al- hmīdbsīūnī, Al- sẖt AL- ilktrūnyā , AL- ṭb‘h ,AL-āūlā - Dār Al- ktb , Al - ‘lmīhllnshrūaltūzī‘, AL-qāhrh, 2008.

-‘bd Al-ftāẖ ẖjāzī, mūkāfẖ jrām AL-kmbūīūtrūaālntrntfī AL- qānūn, AL-‘rbī, AL-nmūdhjī, ṭb‘h1, dār, AL-nhḏh, AL- ‘rbīh, msr, 2009.

-Fāīz, AL-njār, ndhm, AL - m‘lūmāt, AL-Ādārīh, dār AL- ẖ llnshrūaltūzī‘, ‘mān, 2007.

-lmya' AL-klīfh,bnā' ndhām , AL-sjlāt ,AL-ṭbīh, bẖthtkmīliunlnīl, drjh AL-mājstīrfīndhm, AL- m‘lūmāt, jām‘t, AL-nīlīn, 2016..

- mṣbāh, ‘bd, AL-hādī ,AL-dūīk, ndhām, AL-m‘lūmāt, AL-ṣhīh, AL-mhūsbh, wāthrh, ‘lā, AL-qrārāt, AL-ādārīh, ūallṭbīh,: drāshtṭbqīh, ‘lā, mstshā, ghzh, AL-ūrūbī, rsālh, mājstīr, mnshūrh, fī, AL- jām‘h, AL-slāmīh, -ghzh, 2010.

## المراجع الأجنبية:

### أولاً: المراجع الأنجليزية:

- Akan ، Yunus (2021) An Analysis of the Impact of the Values Education Class Over the University Students’ Levels of Acquisition of Moral Maturity and Human Values ، International Journal of Psychology and Educational Studies، 2021، 8 (2)، 38-50.

- A summary of the HIPAA Privacy Rule, prepared by the HHS Office for Civil Rights, is available at http://www. hhs.gov/ocr/privacysummary.pdf (accessed october 13, 2021.

- Benaloh J, Chase M, Horvitz E, Lauter K. Patient controlled encryption: ensuring privacy of electronic medical records. In: Proc ACM workshop on cloud computing security; 2009, p. 103–14.

- Beyer, Karen. (2000). "First Person: Jaffee v. Redmond Therapist Speaks." American Psychoanalyst,Volume 34, no. 3.

- Brodnik, M., L. Rinehart-Thompson and R. Reynolds (2012). Fundamentals of Law for Health Informaticsand Information Management Professionals. Chicago: AHIMA Press. Chapter 1.

- Carey et al,TheGeisingerMyCode community health initiative: an electronic health record–linked biobank for precision medicine research Genet Med, 18 (9) (2016), p. 906.

- Culnan MJ, Williams CC. How ethics can enhance organizational privacy: lessons from the ChoicePoint and TJX data breaches. MIS Quart. 2009;33(4):673–87.

- European Commission, e-Health - making healthcare better for European citizens: an action plan for a European e-Health Area. 2004, European Commission: Brussels.

- Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data.

- MediPro. Advantages and Disadvantages of EMR vs. Paper-Based Records - MediPro. 2019.

- MoradiGh. New dimensions of health-medical information and medical records management. Tehran: Vazhepardaz Publication; 2003.

- MoradiGh. New dimensions of health-medical information and medical records management. Tehran: Vazhepardaz Publication; 2003.

- McWay, Dana. (2010). Legal and Ethical Aspects of Health Information, Third Edition. New York: Cengage Learning. Chapter 9.P.174.

- Mental Health and Developmental Disabilities Confidentiality Act (MHDDCA) (740 ILCS 110). EffectiveJuly 1, 1997. Illinois General Assembly. Retrieved from

- Mental Health and Developmental Disabilities Confidentiality Act (MHDDCA) (740 ILCS 110). EffectiveJuly 1, 1997. Illinois General Assembly.

- Stroetmann K., A.J., Stroetmann V.N. et al. European countries on their journey towards national eHealth infrastructures. 2011.

- Smith T.T. Examining Data Privacy Breaches in Healthcare.

-Tarr, Peter J.(2007) Crossing the digital Rubicon: committing to electronic medical record systems,Community Oncology, Volume 4,Number 5 .

**ثانياً: المراجع الفرنسيـة:**

- Décret n° 2007-960 du 15 mai 2007 relatif à la confidentialité des informationsmédicalesconservées sur support informatiqueoutransmises par voieélectroniqueetmodifiant le code de la santé publique (dispositions réglementaires). https://www.legifrance.gouv.fr.

- Code de la santé publique. Dernièremise à jour des données de cecode : 09 octobre 2021.