| | | |
|---|---|---|
| **نوع الوثيقة:** سياسة المعلومات الصحية | **الرمز الكودي:** DHA/HISHD/PP-11 | **رقم الإصدار : 1** |
| **عنوان السياسة:** حماية البيانات والمعلومات الصحية وخصوصيتها | **تاريخ الإصدار:** 2022/08/10<br>**تاريخ التفعيل:** 2022/10/10<br>**تاريخ المراجعة:** 2027/08/10 | |
| **ملكية الوثيقة:** هيئة الصحة في دبي | | |
| **نطاق التطبيق:** المنشآت الصحية العاملة ضمن نطاق اختصاص وصلاحيات هيئة الصحة في دبي | | |

## 1. التعاريف/الاختصارات

**الدولة:** دولة الإمارات العربية المتحدة

**الهيئة:** هيئة الصحة بدبي

**المكتب:** مكتب الأمارات للبيانات المنشأ بموجب المرسوم بقانون اتحادي رقم (44) لسنة 2021.

**المنشاة:** أي جهة أو مؤسسة صحية داخل الإمارة التي تساهم في تقديم الخدمات الصحية و/أو خدمات الرعاية الصحية المساندة، أو تمويل الرعاية الصحية مثال: شركات التأمين الصحي ووسطاء الضمان الصحي، المستشفى، العيادة أو المركز الطبي، مقدمي خدمات التطبب عن بعد، المختبرات والمراكز التشخيصية،

الصيدليات... الخ

**الإمتثال:** هو اتخاذ ما يلزم من تدابير لتحقيق الالتزام وإظهار وبرهنة هذا الالتزام لمعيار أو تنظيم (دولي أو محلي)

**السرية:** تمثل السرية أحد المكونات الرئيسة الثلاثة لأمن المعلومات، وتعني السرية عدم إتاحة المعلومات أو الكشف عنها لإفراد أو مؤسسات أو ضمن إجراءات غير مصرح لها بذلك وفق أحكام التشريعات السارية.

**الموافقة:** هي الموافقة التي يصرح فيها صاحب البيانات للغير بمعالجة بياناته الشخصية. وتكون الموافقة محددة وواضحة بشكل لا لبس فيه على قبول الشخص بمعالجة بياناته من خلال بيان أو إجراء واضح.

**المتحكم:** هي الجهة التي لديها البيانات والمعلومات الصحية وبحكم النشاط تقوم بتحديد طريقة وأسلوب ومعايير معالجة هذه البيانات والغاية من معالجتها سواءً بمفردها أو بالاشتراك مع أشخاص أو جهات أخرى. في هذه السياسة المتحكم في البيانات والمعلومات الصحية هي المنشاة.

**البيانات:** هي مجموعة منظمة من المعلومات، الوقائع، المفاهيم، التعليمات، المشاهدات، القياسات تكون على شكل أرقام، حروف، كلمات، رموز، صور، فيديوهات، إشارات، أصوات، خرائط أو أي شكل أخر يتم إنشائها أو معالجتها أو تخزينها أو يتم تفسيرها أو تبادلها أو معالجتها من قبل الأفراد أو تكنولوجيا المعلومات والاتصالات.

**المعلومات الصحية:** البيانات الصحية التي يتم معالجتها بحيث تكون واضحة بيّنة سواءً كانت مرئية أو مسموعة أو مقروءة، وذات مرجعية صحية سواء كانت متعلقة بالمنشآت الصحية، مؤسسات التأمين أو

المستفيدين من الخدمات الصحية.

**المعالجة المؤتمتة:** المعالجة التي تتم باستخدام برنامج أو نظام إلكتروني، يعمل بطريقة آلية وتلقائية إما بشكل مستقل كليا دون أي تدخل بشري أو بشكل جزئي بإشراف وتدخل بشري محدود.

**التنميط:** شكل من اشكال المعالجة المؤتمتة بحيث تتضمن استخدام البيانات الشخصية لتقييم جوانب شخصية معينة ومرتبطة بصاحب البيانات، ومن بينها تحليل او توقع الجوانب المتعلقة بادائه او وضعه المالي او صحته او تفضيلاته الشخصية او اهتماماته او سلوكه او مكانه

**تقييم حماية البيانات:** تقييم المخاطر المحتملة على خصوصية وسرية البيانات والمعلومات الصحية والإجراءات والتدابير المقترحة للحد من المخاطر المحتملة على حماية البيانات والمعلومات الصحية وهي عملية مُصممّة لتحديد المخاطر التي قد تنشأ عن معالجة المعلومات الصحية، وكيفية تقليل أو تفادي هذه المخاطر في مرحلة مبكرة من المعالجة وإلى أقصى حد ممكن.

**مسؤول حماية البيانات**: أي شخص طبيعي أو اعتباري يتم تعيينه من قبل المتحكم أو المعالج يتولى مهام التأكد من مدى امتثال الجهة التي يتبعها لضوابط واشتراطات وإجراءات وقواعد معالجة المعلومات الصحية المنصوص عليها وفقاً للقانون الاتحادي رقم 45 لسنة 2021 للدولة بشأن حماية البيانات الشخصية والتأكد من سلامة أنظمتها وإجراءاتها من اجل تحقيق الالتزام بأحكامه

**صاحب البيانات:** الشخص الطبيعي موضوع البيانات والمعلومات الصحية.

**الإفصاح ومشاركة البيانات والمعلومات الصحية:** هو نقل أو مشاركة البيانات والمعلومات الصحية مع طرف ثالث.

**التخلص**: يشير إلى التدابير والإجراءات اللازمة لتحقيق إتلاف أو نقل آمن لأصول البيانات والمعلومات الصحية ليتم حفظها بشكل كامل. يتم تقديم شهادة نقل لهذه البيانات كإثبات على عملية النقل (ويمكن أن تمثل دليل التخلص).

**الإتلاف:** يشير إلى التدابير والإجراءات اللازمة لتحقيق إتلاف آمن وبشكل يحفظ سرية أصول البيانات والمعلومات الصحية التي يتم إتلافها مع إثبات هذا الإتلاف. يمثل هذا الإتلاف أصول البيانات والمعلومات الصحية التي لا قيمة لأرشفتها، ولم يعد هناك حاجة للاحتفاظ بها لفترة أطول.

**الطرف الثالث**: يقصد بها الأفراد أو المؤسسات التي تتعامل مع الجهة الصحية من خلال علاقة عمل أو لديها صلاحية الوصول إلى البيانات والمعلومات الصحية لهذه الجهة.

**تبادل المعلومات الصحية**: الوصول إلى المعلومات الصحية، تبادلها، نسخها وتصويرها ونقلها، تخزينها ونشرها والإفصاح عنها أو نقلها.

**الحوادث:** المخالفات أو التهديدات المتوقعة بانتهاك سياسات أمن المعلومات، أو سياسات الاستخدام المقبول أو معايير الأمن المعلوماتي للمتحكم بالبيانات والمعلومات الصحية.

**الاستخدام الأولي:** ويشمل استخدام البيانات والمعلومات الصحية التي يتم جمعها من خلال المنشأة وفي سياق الرعاية الصحية المقدمة للمريض وللأغراض الأساسية لتقديم الرعاية الصحية والعلاج للمريض.

**الاستخدام الثانوي (غير المباشر) للمعلومات الصحية:** استخدام المعلومات الصحية لأغراض أخرى غير رعاية المريض، على سبيل المثال: البحث، والصحة العامة، والتدقيق السريري وتحسين الجودة، ومبادرات الأمن والسلامة، إجراءات إعتماد المنشآت والتقييم، وجود شكوى طبية، المقاضاة أو الدفاع عن دعوى أو

شكوى قانونية وأغراض التسويق. وقد تستكمل بعض هذه الاستخدامات الثانوية بشكل مباشر احتياجات الاستخدام الأولي لها، مثال: مطالبات التأمين، الإجراءات الإدارية والتنظيمية المرتبطة بالمنشأة.

**المعلومات الصحية المحمية:** هي التي تتضمن أي من المعرّفات الثمان عشرة (18) التالية:

- الاسم (الاسم الكامل بما يتوافق مع جواز السفر أو الهوية الإماراتية)
- العنوان (جميع المعالم الجغرافية)
- جميع عناصر التواريخ (بخلاف السنوات) المتعلقة بالفرد (متضمنة: تاريخ الميلاد وتاريخ التنويم وتاريخ الخروج وتاريخ الوفاة والعمر بالتحديد – في حال كان أكبر من 89 عامًا).
- أرقام الهاتف
- رقم الفاكس
- عنوان البريد الإلكتروني
- رقم الهوية الإماراتي
- رقم الملف الصحي
- رقم بوليصة التأمين الخاصة بكل مؤمن
- رقم الحساب البنكي
- رقم رخصة القيادة

- مُعرّفات المركبات (بما في ذلك الأرقام التسلسلية وأرقام لوحات السيارات)
- مُعرّفات الجهاز أو الأرقام التسلسلية
- مُعرّفات المواقع الإلكترونية (URLs)
- أرقام عناوين بروتوكول الإنترنت(IP)
- مُعرّفات القياسات الحيوية، بما في ذلك بصمات الأصابع وبصمة العين والصوت
- صور فوتوغرافية كاملة الوجه وأي صور مماثلة
- أي رقم تعريفي موحد آخر أو خاصية أو رمز.

**المعالجة:** أي عملية يتم إجراؤها على البيانات والمعلومات الصحية مثل:

- الإفصاح عن طريق النقل، النشر أو الإتاحة بأي وسيلة أخرى
- الموائمة أو الدمج
- الجمع، التسجيل، الترتيب، التنظيم أو التخزين (على سبيل المثال ضمن نظام الملفات)
- التكييف أو التعديل
- الاسترجاع، الاستشارة أو الاستخدام
- حجب البيانات، إتلافها أو محوها

**المعالج:** المنشأة أو الشخص الطبيعي الذي يعالج المعلومات الصحية نيابة عن المتحكم ويقوم بمعالجتها وفقاً لتوجيهه وتعليماته.

**التسمية المستعارة:** المعالجة التي يتم إجراؤها على المعلومات الصحية بطريقة تؤدي إلى عدم إمكانية ربط أو تنسيب هذه المعلومات بصاحبها دون استخدام معلومات إضافية. شريطة أن تكون تلك المعلومات الإضافية محفوظة بشكل مستقل وآمن ووفقاً للتدابير والإجراءات التقنية والتنظيمية اللازمة لضمان عدم ارتباط البيانات الشخصية بشخص طبيعي محدد أو يمكن التعرف عليه.

**المصلحة العامة:** الظروف الاستثنائية التي تسوغ إبطال حق الفرد في السرية من أجل خدمة أوسع لمصلحة المجتمع.

**طلب الوصول للمعلومات الصحية:** هو طلب الوصول للمعلومات الصحية والذي يسمح للشخص صاحب البيانات بالحصول على سجلات المعلومات الصحية التي تحتفظ بها المنشأة.

## 2. الغرض

2.1. تحديد شروط وضوابط هيئة الصحة في دبي لضمان حماية وسلامة البيانات والمعلومات الصحية وسريتها وبما يتوافق مع القوانين السارية بدولة الإمارات العربية المتحدة، والأطر التشريعية / التنظيمية المُطبقة في إمارة دبي.

2.2. التحقق من أن كافة المنشآت الصحية العاملة ضمن نطاق اختصاص وصلاحيات هيئة الصحة في دبي توفر بيئة آمنة لإدارة البيانات؛ وعلى وجه التحديد المعلومات الصحية - والتي يطلق عليها

أيضًا "المعلومات الصحية المحمية".

2.3. التعريف بواجبات ومسؤوليات المنشآت الصحية العاملة ضمن نطاق اختصاص وصلاحيات هيئة الصحة في دبي لتحقيق شروط وضوابط حماية وسلامة البيانات والمعلومات الصحية وسريتها.

2.4. ضمان الحفاظ على سرية وخصوصية البيانات والمعلومات الصحية المتعلقة بإفراد المجتمع من خلال توفير أطر حوكمة مناسبة لإدارة هذه البيانات والمعلومات وحمايتها على الوجه الأمثل.

2.5. تحديد الحقوق والواجبات لكافة الأطراف المعنية التي تتعامل مع البيانات والمعلومات الصحية في إمارة دبي.

## 3. مجال التطبيق .

3.1. المنشآت الصحية العاملة ضمن نطاق اختصاص وصلاحيات هيئة الصحة في دبي

3.2. البيانات والمعلومات الصحية التي يتم التعامل معها من قبل المنشآت الصحية الواقعة ضمن نطاق اختصاص وصلاحيات هيئة الصحة في دبي.

3.3. المعلومات الصحية، وكما تم تعريفها من قبل القانون رقم (2) لسنة 2019بشأن استخدام تقنية المعلومات والاتصالات في المجالات الصحية في الدولة بجميع أشكالها، بالإضافة إلى التطبيق الأساسي والتكنولوجيا والبنية التحتية المادية والتي تدعم معالجتها وتخزينها وتداولها ومشاركتها. ويشمل ذلك على سبيل المثال لا الحصر:

3.3.1. المعلومات الصحية والسجلات الإدارية (مثال الموارد البشرية، سجلات الشكاوى،

السجلات الإدارية المتعلقة بالمهام التشغيلية للمنشأة... الخ).

3.3.2. البيانات المُعرفة والغير قابلة للتعريف.

3.3.3. البيانات التي يمكن الوصول إليها للاستخدام الأولي أو الثانوي.

3.3.4. البيانات الورقية أو الرقمية.

3.3.5. أنظمة سجل البيانات المُهيّكلة (الورقية والإلكترونية)

3.3.6. نقل البيانات (الفاكس والبريد الإلكتروني والبريد والهاتف)

3.4. جميع أنظمة المعلومات التي تم شراؤها أو تطويرها أو إدارتها أو استخدامها من قبل المنشأة المعنية.

3.5. المستخدمين الذين لديهم صلاحية الوصول إلى البيانات "المملوكة كليًا أو جزئيًا" للمنشأة المعنية واستخدامها في القطاع الصحي في إمارة دبي؛ بما في ذلك الموظفين المصرح لهم ومزودي الخدمة والشركاء في تقديم الخدمة على نطاق أوسع وكلما اقتضت الحاجة ذلك.

## 4. بيان السياسة

**4.1.** تعد سياسة حماية البيانات والمعلومات الصحية وخصوصيتها جزءًا لا يتجزأ من نهج الهيئة. ويجب قراءة هذه السياسة جنبًا إلى جنب مع السياسات والمعايير ذات الصلة والصادرة عن أو السارية لدى قطاع التنظيم الصحي التابع للهيئة.

**4.2.** السياسة راعت ما نصت عليه التشريعات السارية بشأن البيانات والمعلومات الصحية، وآلية معالجتها وتداولها. حيث حرصت الهيئة من خلال هذه السياسة المؤامة مع كافة القوانين واللوائح التشريعية السارية بشأن المعلومات الصحية المذكورة أدناه:

4.2.1.القانون الاتحادي للدولة رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية والتي لها تأثير مباشر على تدابير حماية المعلومات الصحية:

https://www.dha.gov.ae/en/licensing-regulations-laws

4.2.2.قرار مجلس الوزراء رقم (32) لسنة 2020 بشأن اللائحة التنفيذية للقانون الاتحادي رقم (2) لسنة 2019 في شأن استخدام تقنية المعلومات والاتصالات في المجالات الصحية:

https://www.dha.gov.ae/en/licensing-regulations-laws

4.2.3.القرار الوزاري رقم (51) لسنة 2021 بشأن الحالات التي يجوز فيها تخزين أو نقل البيانات والمعلومات الصحية إلى خارج الدولة: https://www.dha.gov.ae/en/licensing-regulations-laws

4.2.4.سياسة تصنيف أصول البيانات والمعلومات في المجالات الصحية على مستوى إمارة دبي: https://nabidh.ae/#/comm/policies.

ونتيجة لذلك، فأن اللوائح والتنظيمات الأكثر تخصصاً / تفصيلاً هي التي تسود ويُتبع ما هو أكثر إلزاماً.

**4.3. ضوابط الهيئة بشأن معالجة المعلومات الصحية المحمية:**

تلتزم الهيئة بالمبادئ التالية والمستمدة من القوانين والتشريعات السارية في الدولة بشأن معالجة المعلومات الصحية المحمية، وتنطبق هذه المبادئ على استخدام المعلومات الصحية المحمية داخل المنشآت الصحية وعند مشاركتها مع جهات أو أفراد آخرين.

ويعد الإمتثال لهذه الضوابط والشروط هو الأساس ويؤدي عدم الامتثال لهذه القواعد إلى اتخاذ

الإجراءات التنظيمية المناسبة.

4.3.1. **العدالة والقانونية والشفافية:**

أن تكون معالجة المعلومات الصحية المحمية عادلة وشفافة ومشروعة وتتوافق مع أحكام التشريعات السارية.

4.3.2. **غرض المعالجة:**

أ. يجب أن يتم جمع المعلومات الصحية المحمية لأغراض الاستخدام الأولية بطريقة محددة، واضحة وشرعية واقتصار المعالجة على الغرض المحدد لها فقط.

ب. اقتصار جمع أي معلومات صحية محمية تم تقديمها أو تلقيها لغرض واضح ومحدد، وألا يتم معالجتها في أي وقت لاحق على نحو يتنافى مع ذلك الغرض.

ج. في حال استخدام المنشأة للمعلومات الصحية المحمية لأغراض أخرى غير الاستخدام الأولي، فإنه يجب اتباع قانون تكنولوجيا المعلومات والاتصالات في المجال الصحي في الدولة بهذا الشأن: -

1.ج. يجب تبرير الغرض (الأغراض) من استخدام المعلومات الصحية المحمية للاستخدام الثانوي.

2.ج. يجب تسجيل الغرض من الاستخدام الثانوي للمعلومات الصحية المحمية.

3.ج. يجب الحصول على الموافقات الأخرى المطلوبة من قبل الهيئة بشأن الاستخدام

الثانوي للمعلومات الصحية المحمية وذلك بالتواصل عبر البريد الإلكتروني لإدارة المعلوماتية والصحة الذكية في الهيئة: HISH@dha.gov.ae.

4.3.3. **خفض حجم البيانات:**

أ. يجب أن تكون المعلومات الصحية المحمية كافية وذات صلة وليست كبيرة على نحو مفرط، وأن تكون مقتصرة على ما هو ضروري بالأغراض التي تتم معالجتها من أجلها.

ب. يجب الاحتفاظ المعلومات الصحية المحمية في شكل يسمح بتحديد موضوعات البيانات لفترة لا تزيد عما هو ضروري للأغراض التي تتم معالجة المعلومات الصحية من أجلها.

4.3.4. **الدقة:**

أ. على المنشأة الصحية التحقق من إن المعلومات الصحية المحمية دقيقة وصحيحة وأن تخضع للتحديث متى اقتضى الأمر ذلك.

ب. يجب على المنشأة توفير التدابير والإجراءات المطلوبة لضمان محو أو تصحيح المعلومات الصحية غير الصحيحة مباشرة.

4.3.5. **النزاهة، السرية والأمن**

على المنشأة ضمان النزاهة والسرية في التعامل مع ال المعلومات الصحية المحمية في كافة الظروف والأوقات

4.3.6. **الاحتفاظ بالمعلومات الصحية المحمية:**

أ. وفقاً لما نصت عليه التشريعات السارية في الدولة بشكل عام وإمارة دبي والهيئة بشكل خاص، يتم إجراء المعالجة للمعلومات الصحية وفق الغرض والمدة المحددة لها.

ب. لا يجوز الاحتفاظ بالمعلومات الصحية المحمية بعد استنفاذ الغرض من معالجتها وعلى المنشأة الصحية اتخاذ التدابير اللازمة في التخلص من المعلومات الصحية بشكل آمن بعد انقضاء مدة المعالجة.

ج. يتم تحديد الإطار الزمني للحفاظ على المعلومات الصحية المحمية التي تم معالجتها وفقاً للوائح التنظيمية والسياسات المعتمدة من قبل الهيئة.

**4.4.خصوصية المعلومات الصحية المحمية:**

4.4.1. يجب حماية سرية المعلومات الصحية المحمية في جميع الظروف وفقاً لما نصت عليه التشريعات السارية في الدولة بشكل عام وإمارة دبي والهيئة بشكل خاص.

4.4.2. أثناء إدارة / معالجة المعلومات الصحية المحمية، على المنشأة ضمان الحفاظ على المعايير التقنية / التنظيمية المناسبة لحماية سلامة البيانات والمعلومات الصحية وسريتها، وبما في ذلك الحماية من:

أ. الوصول غير المصرح به

ب. المعالجة غير القانونية

ج. فقدان البيانات والمعلومات الصحية العرضي / التلف/ التدمير

4.4.3. يجب أن تتضمن عقود عمل التوظيف على شرط يتعلق بحوكمة المعلومات/ حماية البيانات. كما تنطبق نفس القاعدة على العقود المبرمة مع الطرف الثالث / الجهات الأخرى، وعقود التوظيف المؤقتة.

4.4.4. يتوجب على المنشآت توفير "اتفاقية سرية المعلومات" والتي تُلزم الموظفين غير التابعين للمنشأة بالتوقيع عليها قبل القيام بأي أعمال مرتبطة بالبيانات والمعلومات الصحية المملوكة للمنشأة أو بالنيابة عنها.

4.4.5. يكون الزامياً على المنشأة توفير خدمة حفظ سرية وخصوصية البيانات والمعلومات الصحية المقدمة. ويجب إجراء التحقيقات اللازمة حال وجود أي مخالفة لحفظ هذه السرية والتي يجب أن تؤدي إلى اتخاذ الإجراءات النظامية اللازمة ضد المتسببين في هذا الانتهاك.

**4.5. الخصوصية عبر التصميم -حماية البيانات والمعلومات الصحية الافتراضية**

4.5.1. يتوجب توفير ما يلزم لحماية البيانات والمعلومات الصحية تلقائياً عند بداية أي مشروع جديد، خدمة، عقد أو عملية جديدة.

4.5.2. تضمين مبادئ حماية البيانات والمعلومات الصحية في كل جانب من جوانب أنشطة معالجة المعلومات الصحية المحمية. ويتضمن ذلك تطبيق مبادئ سلامة البيانات وحماية حقوق الأفراد، مثال ذلك: تقليص حجم البيانات، التسمية المستعارة (طمس الهوية) وتحديد الغرض على النحو المنصوص عليه في هذه السياسة.

**4.6. حقوق صاحب البيانات في سرية البيانات والمعلومات الصحية:**

نص القانون الاتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية على حقوق أصحاب البيانات التي تخضع للمعالجة. وعليه يتوجب على جميع الأطراف المعنية:

4.6.1. الحصول على الموافقة التي يصرح فيها صاحب البيانات للغير بمعالجة المعلومات الصحية المحمية الخاصة به:

أ. دون الإخلال بالتشريعات السارية، يتوجب على الشخص المسؤول عن تبادل البيانات والمعلومات الصحية وتداولها إتخاذ الإجراءات والتدابير المناسبة للحفاظ على سريتها وخصوصيتها وضمان عدم استخدامها لأغراض غير صحية وأخذ الموافقة اللازمة من صاحب البيانات.

4.6.2. معرفة أنواع البيانات والمعلومات الصحية التابعة له التي يتم معالجتها:

أ. الغرض من المعالجة

ب. المنشآت أو الجهات التي سيتم مشاركتها بياناته ومعلوماته الصحية (داخل وخارج الدولة) والتي ستقوم بمعالجة هذه البيانات والمعلومات الصحية.

4.6.3. تقييد / إيقاف معالجة المعلومات الصحية المحمية التي تتم عن طريق المعالج، ووفق ما نصت عليه المواد رقم (16، 17، 18) من القانون الاتحادي رقم 45 لسنة 2021 بشأن حماية البيانات الشخصية.

4.6.4. معرفة تدابير الحماية الخاصة بالمعالجة أثناء نقل البيانات والمعلومات الصحية بين الجهات المعنية (داخل وخارج الدولة).

4.6.5. إخبار صاحب البيانات بضوابط المعالجة، الإطار الزمني للتخزين/ الأرشفة المعلومات الصحية.

4.6.6. القرارات المتخذة بناءً على المعالجة المؤتمتة المعلومات الصحية الخاصة به.

4.6.7. الكشف عن طبيعة المعلومات الصحية التي يتم مشاركتها مع جهات أخرى حسب الضرورة. ولا يتعارض هذا الحق في إعاقة صاحب البيانات من الاستفادة من خدمات الرعاية الصحية.

4.6.8. طلب نقل المعلومات الصحية كلما أمكن ذلك من الناحية التقنية.

4.6.9. طلب تصحيح المعلومات الصحية غير الدقيقة أو استكمال نواقص البيانات غير المكتملة. ويتم تقييم هذه الطلبات والرد عليها من قبل المنشأة خلال 5 أيام عمل.

4.6.10. إخطار صاحب البيانات والمعلومات الصحية بمخالفة الجهة المسؤولة عن معالجة المعلومات الصحية وطريقة إبلاغه عن هذه المخالفة.

4.6.11. دون الإخلال بالتشريعات السارية في الدولة وما تتطلبه المصلحة العامة، يحق لصاحب البيانات والمعلومات الصحية طلب تقييد/ إيقاف معلوماته الصحية من عملية المعالجة، وذلك وفقاً للحالات التي تم تعريفها في المادة رقم (15) من القانون الاتحادي رقم 45 لسنة 2021 بشأن حماية البيانات الشخصية.

4.6.12. حق الوصول إلى المعلومات الصحية الخاصة به عن طريق " طلب الوصول للمعلومات الصحية" والذي يمكنه من الرجوع إلى معلوماته الصحية والحصول على نسخة من

سجلات المعلومات الصحية مثال: الملف الصحي، تفاصيل مزود الخدمة الصحية، سجلات الفواتير أو تفاصيل خطة العلاج، الدفع، مطالبات التأمين. كما يتعين على المنشأة الآتي:

أ. توثيق الطلب الشفهي أو الكتابي المقدم من قبل صاحب البيانات.

ب. الرد على طلب الوصول للمعلومات الصحية في غضون شهر (30 يوم) من استلامه.

ج. التحقق من تحديث الملفات الصحية الإلكترونية عند تلقي هذه الطلبات وكلما اقتضى الأمر ذلك.

د. توثيق كافة الاتصالات والوثائق المرتبطة بهذه الطلبات لفترة زمنية محددة وفقاً لما حدده القانون الاتحادي رقم (2) لسنة 2019 في شأن استخدام تقنية المعلومات والاتصالات في المجالات الصحية والشروط والضوابط المطبقة من قبل الهيئة.

4.6.13. الحق في التقدم بشكوى إلى جهة الإشراف المعنية (الهيئة).

**4.7. أنظمة تكنولوجيا المعلومات:**

4.7.1. يتوجب على المنشأة توفير أنظمة تكنولوجيا المعلومات بضوابط مناسبة تمنع فقدان البيانات والمعلومات الصحية أو السماح بمعالجات غير قانونية أو الوصول غير الشرعي لها.

4.7.2. توفير المنشأة سياسة داخلية لأمن المعلومات تتضمن إرشادات مفصلة عن أمن النظام المعلوماتي الخاص بها بما في ذلك الحد الأدنى من معايير ضوابط الوصول إلى البيانات

والمعلومات الصحية.

### 4.8. الوصول إلى المعلومات الصحية المحمية/ استخدام المعلومات الصحية

4.8.1. على المنشآت الصحية تطوير وتطبيق سياسات وإجراءات خاصة لتقييد الوصول واستخدام المعلومات الصحية المحمية وبناءً على تحديد الأدوار للموظفين، المتدربين، مقدمي الخدمة والطرف الثالث/ الأطراف الأخرى المعنية بها.

4.8.2. يجب أن تحدد السياسات والإجراءات النقاط الآتية:

أ. الأشخاص أو الفئات ضمن المنشأة والذين لديهم صلاحية الوصول إلى المعلومات الصحية المحمية لأداء واجباتهم.

ب. فئة المعلومات الصحية المحمية التي يلزم الوصول إليها.

ج. الحالات التي تتطلب فيها الوصول للمعلومات الصحية المحمية لأداء مهام العمل.

4.8.3. على المستخدمين الوصول للمعلومات الصحية المحمية التي لديهم تصريح من قبل أصحابها بالوصول إليها فقط ولأغراض محددة.

4.8.4. الوصول إلى أي سجلات بطريقة غير شرعية / مصرح به هو أمر محظور وغير قانوني.

4.8.5. يحظر على الموظفين والذين لا يشكلون جزءاً من فريق الرعاية من الوصول إلى المعلومات الصحية المحمية المتوفرة في الملفات الصحية المتعلقة بالأقارب/ الأصدقاء أو زملاء العمل.

4.8.6. امتناع الموظفين عن محاولة استخدام الأنظمة الإلكترونية التي لم يتم تدريبهم عليها أو مصرح لهم بالوصول إليها.

4.8.7. على الموظفين القائمين على أنظمة المعلومات الصحية عدم السماح لأخرين بالوصول إليها عن طريق استخدام بيانات تسجيل الدخول الخاصة بهم، أو مشاركتهم كلمات المرور حيث يعد هذه الفعل مخالفة تأديبية وانتهاكاً خطيراً للقوانين والتشريعات السارية بهذا الشأن.

4.8.8. على المنشأة إجراء تدقيق دوري للتحقق من سلامة الإجراءات المتبعة في الوصول إلى المعلومات الصحية، وفي حال تبين وجود مخالفة إتباع الشروط والضوابط من قبل أي من الموظفين المسؤولين عن النظام، فإنه يجب اتخاذ الإجراءات التأديبية المناسبة.

4.8.9. وفقا للتشريعات السارية في الدولة بشكل عام وإمارة دبي والهيئة بشكل خاص، فإن الدخول غير المصرح به للنظم المعلوماتية بما في ذلك القرصنة واستخدام بيانات أخرين يعد فعلاً مجرماً ويعرض مرتكبه للمساءلة القانونية.

**4.9. إستمرارية الأعمال/ خطة استعادة البيانات والمعلومات الصحية**

4.9.1. على المنشأة ضمان توفير كلا من خطة استمرارية الأعمال وكذلك خطة استعادة البيانات والمعلومات الصحية عند حدوث طارئ ما لأصول المعلومات المتوفرة لديه.

4.9.2. يتوجب على المنشأة التحقق من فعالية الخطة الموضوعة بشكل دوري وبهدف الحفاظ على سلامة وتوفر المعلومات الصحية.

**4.10. معالجة المعلومات الصحية المحمية داخل المنشأة:**

4.10.1. يجب أن يتم المعلومات الصحية المحمية داخل المنشأة بشكل قانوني، ووفقاً لما تنص عليه التشريعات السارية في الدولة بشكل عام وإمارة دبي والهيئة بشكل خاص.

4.10.2. يجب أن تتم معالجة البيانات والمعلومات الصحية (لأهداف تخص تقديم الرعاية الصحية لصاحب البيانات) في إطار من السرية والخصوصية.

4.10.3. على المنشأة إبلاغ أصحاب البيانات ومستخدمي الرعاية الصحية عن القرارات المتخذة بشأن كيفية استخدام المعلومات الصحية المحمية الخاصة بهم والجهة التي سيتم مشاركتها هذه المعلومات.

4.10.4. يجب الحصول على موافقة صاحب البيانات على إستخدام المعلومات الصحية الخاصة به لغرض ثانوي- معالجة إضافية.

4.10.5. عند إجراء المعالجة نيابة عن المنشأة الصحية (المتحكم) يجب على المنشأة استخدام المعالجات التي تضمن توفير التدابير الفنية والتنظيمية اللازمة والتي تلبي متطلبات هذه السياسة وتضمن حماية حقوق الشخص صاحب البيانات.

4.10.6. في حال إشراك معالج أخر، على المعالج الأساسي الحصول على أذن أو تصريح كتابي واضح محدد أو عام من قبل المنشأة (بصفته المتحكم في المعلومات الصحية)، قبل البدء في عملية المعالجة يوضح فيها الالتزامات والمسؤوليات.

4.10.7. في حال التصريح الكتابي العام، على المعالج إبلاغ وحدة التحكم بأي تغييرات يتم القيام

بها وتتعلق بإضافة أو استبدال معالجات أخرى، وبالتالي إعطاء المنشأة الفرصة (بصفته المتحكم في المعلومات الصحية) في التحقق من هذه التغييرات.

**4.11. معالجة المعلومات الصحية المحمية من خلال نظام نابض لتبادل المعلومات الصحية**

4.11.1. يتوجب على المنشأة الحصول على موافقة الشخص صاحب البيانات للوصول إلى معلوماته الصحية المحمية عبر نظام "نابض".

أ. يجب أن يكون نموذج الموافقة واضح، بسيط، غير مبهم وسهل الفهم.

ب. يجوز أن يكون نموذج الموافقة على شكل ورقي أو الكتروني.

ج. يجب أن يحتوي النموذج على جزء خاص بشأن طلب "تقييد وإيقاف" المعالجة وضمان سهولة التطبيق.

د. الموافقة الممنوحة صالحة مدى الحياة، ما لم يقرر صاحب البيانات الخروج من منظومة "نابض".

4.11.2. صاحب البيانات يجب أن يكون لديه الحرية ل "إلغاء الاشتراك" من منظومة "نابض" في أي وقت؛ علما بأن إلغاء الاشتراك لن يؤثر على المعلومات الصحية المعالجة مسبقًا.

**4.12. التزامات المعالج للمعلومات الصحية المحمية:**

4.12.1. يتوجب على معالج المعلومات الصحية التقيد بالقوانين والتشريعات السارية في الدولة وسياسات الهيئة بشأن المعلومات الصحية وخصوصيتها.

4.12.2. يتوجب على معالج المعلومات الصحية تطبيق الإجراءات والتدابير التقنية والتنظيمية المناسبة لحماية المعلومات الصحية أثناء المعالجة.

4.12.3. على المعالج إجراء معالجة البيانات والمعلومات الصحية وفق الغرض والوقت الزمني المحدد له، وفي حالة تجاوزت المعالجة المدة الزمنية المحددة، على المعالج إخطار المنشأة (بصفتها المتحكم في المعلومات الصحية) للموافقة بتمديد الفترة الزمنية.

4.12.4. على المعالج محو / إزالة المعلومات الصحية بعد انقضاء مدة المعالجة أو تسليمها للمنشأة بعد انتهاء المدة الزمنية المحددة للمعالجة المعلومات الصحية.

4.12.5. يتوجب على المعالج عدم الإفصاح عن أي من المعلومات الصحية أو نتائج المعالجة لأي طرف من الأطراف، إلا في الأحوال المصرح بها قانوناً.

4.12.6. يتوجب على المعالج توفير سجل خاص للإجراءات المتخذة بشأن معالجة المعلومات الصحية.

### 4.13. معالجة المعلومات الصحية المحمية دون موافقة صاحب البيانات

وفقاً للقانون الاتحادي رقم (2) لسنة 2019 في شأن استخدام تقنية المعلومات والاتصالات في المجالات الصحية والقانون الاتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية، ودون الإخلال بأية تشريعات سارية، يجب على كل من يتعامل مع المعلومات الصحية المحمية المحافظة على سريتها وخصوصيتها. وعدم استخدامها لغير الاستخدام الأولي دون موافقة خطية من المريض، باستثناء أي من الحالات الآتية:

4.13.1. المعلومات الصحية التي تطلبها شركات التأمين الصحي أو الأطراف الأخرى من مزودي الرعاية الصحية ولأغراض التدقيق، الموافقة أو التحقق من الاستحقاقات المالية المتعلقة بتلك الخدمات.

4.13.2. أغراض البحث العلمي والسريري، شريطة عدم الكشف عن هوية صاحب البيانات ومراعاة الأخلاقيات والقواعد الخاصة بالبحوث العلمية.

4.13.3. أن تكون المعالجة ضرورية لإتخاذ الإجراءات الوقائية والعلاجية المتعلقة بالصحة العامة مثال: الأمراض السارية والأوبئة وتهديدات الأمراض المتنقلة أو للحفاظ على صحة وسلامة صاحب البيانات أو أي أشخاص أخرين على اتصال به.

4.13.4. بناءً على طلب الجهات القضائية المختصة.

4.13.5. بناءً على طلب الهيئة ولأغراض الرقابة والتفتيش والمحافظة على الصحة العامة.

4.13.6. أن تكون المعالجة مرتبطة بالمعلومات الصحية التي أصبحت متاحة ومعلومة من قبل صاحب البيانات.

4.13.7. أن تكون المعالجة ضرورية لممارسة صاحب البيانات حقوقه المقررة قانوناً من إجراءات المطالبة بالحقوق والدعاوى القانونية أو الدفاع عنها أو الدعاوى القانونية المحتملة مثل الشكوى إلى الجهة التنظيمية ضد المنشأة أو المتحكم في المعلومات الصحية أو موظفيها أو أي من الإجراءات القضائية أو الأمنية.

4.13.8. أن تكون المعالجة ضرورية لأغراض قيام المتحكم (المنشأة) بالتزاماته وامتثاله للقوانين

والتشريعات ذات الصلة.

4.13.9. أن تكون المعالجة ضرورية لأغراض الطب الوقائي أو المهني ولتقييم قدرة الموظف على العمل، التشخيص الطبي، توفير الرعاية الصحية أو الاجتماعية أو العلاج أو إدارة أنظمة وخدمات الرعاية الصحية أو الاجتماعية.

4.13.10. لضمان معايير عالية لجودة وسلامة الرعاية الصحية والمنتجات الطبية أو الأجهزة الطبية وفقًا للقوانين المعمول بها في الدولة والتنظيمات المعتمدة من قبل الهيئة.

4.13.11. لأغراض قيام المتحكم أو صاحب البيانات بالتزاماته ومباشرة حقوقه القانونية في مجال التوظيف أو الضمان الاجتماعي أو القوانين المعنية بالحماية الاجتماعية.

4.13.12. لغرض تنفيذ عقد يكون صاحب البيانات طرفاً فيه أو لإتخاذ إجراءات بناءً على طلب صاحب البيانات بهدف إبرام عقد/ تعديله أو إنهائه.

**4.14. الإفصاح ومشاركة المعلومات الصحية المحمية مع طرف ثالث "داخل الدولة"**

4.14.1. في حال طلبت المنشأة من طرف ثالث، داخل الدولة بمعالجة المعلومات الصحية بالنيابة عنها، فإنه يجب توقيع اتفاقية / عقد مشاركة البيانات.

4.14.2. يجب أن تتضمن الاتفاقية/ العقد بنوداً واضحة لتحديد مسؤوليات ضمان حماية البيانات والمعلومات الصحية والسرية وبما يتوافق مع القوانين والتشريعات السارية في الدولة والتنظيمات المتبعة من قبل الهيئة. وفي حال عدم وجود هذا البند بشكل في اتفاقية / عقد مشاركة البيانات، فإنه يجب على مزود الخدمة تقديم اتفاقية عن سرية البيانات

والمعلومات الصحية والتوقيع عليها.

4.14.3. على المنشأة التأكد من قيام المعالج باتخاذ الإجراءات والتدابير التقنية والتنظيمية المناسبة لحماية وتأمين سرية البيانات والمعلومات الصحية.

4.14.4. التزام الطرف الثالث (على سبيل المثال: معالج البيانات) بكافة ضوابط وشروط حماية وسرية المعلومات الصحية حتى بعد انتهاء العقد.

4.14.5. ضمان المنشأة أن المعلومات الصحية المستلمة من / أو تم تبادلها مع طرف ثالث هي معلومات محمية ومحفوظة وفق التشريعات السارية في الدولة بشكل عام وإمارة دبي والهيئة بشكل خاص، ومنها على سبيل المثال لا الحصر:

أ. سياسة تصنيف أصول البيانات والمعلومات في المجالات الصحية على مستوى إمارة دبي:

https://nabidh.ae/#/comm/policies

ب. متطلبات ترخيص المنصة الرقمية في الهيئة:

Online Licencing (Sheryan) – DHA

ج. معايير التطبب عن بعد:

DHA Telemedicine Standards

4.14.6. إتخاذ التدابير والإجراءات التقنية اللازمة لضمان حماية المعلومات الصحية المحمية والمنقولة للمعالجة خارج المنشأة وضمن الدولة، وتشفيرها على نحو آمن أثناء عملية

النقل.

4.14.7. ضمان تشفير كافة الوسائط الإلكترونية المحمولة عند الحاجة إلى نقل بيانات/ سجلات المعلومات الصحية المحمية عبر أي من الوسائط الإلكترونية. كما يجب تنفيذ هذه العملية بشكل صارم للحفاظ على سلامة وسرية هذه المعلومات.

4.14.8. حيثما اقتضت الحاجة بنقل المعلومات الصحية المحمية الكترونياً، يجب الالتزام بإجراءات التحكم في الوصول إلى البيانات والمعلومات الصحية والمتعلقة بالخصوصية والأمان والسرية (مثال: كلمة المرور للبوابات الإلكترونية، بروتوكول طبقة المقابس الأمنة).

4.14.9. يجب عدم الاحتفاظ بالمعلومات الصحية المحمية لفترة تزيد عما هو ضروري للأغراض التي تتم معالجة المعلومات الصحية من أجلها من قبل الطرف الثالث.

**4.15.نقل ومشاركة المعلومات الصحية المحمية خارج دولة الإمارات العربية المتحدة**

4.15.1. لا يجوز نقل المعلومات الصحية المحمية لأي دولة أو إقليم خارج الدولة، بإستثناء المعلومات الصحية المحمية التي تقع ضمن فئة إعفاءات القانون الاتحادي للقانون الاتحادي رقم (2) لسنة 2019 في شأن استخدام تقنية المعلومات والاتصالات في المجالات الصحية:

أ. الالتزام بشروط وضوابط قرار مجلس الوزراء رقم (51) لسنة 2021 بشأن الحالات التي يجوز فيها تخزين أو نقل البيانات والمعلومات الصحية خارج الدولة الحالات التي يجوز فيها تخزين أو نقل البيانات والمعلومات الصحية إلى خارج الدولة

ب. الحصول على موافقة الهيئة وذلك وفقاً لسياسة تصنيف أصول البيانات والمعلومات في المجالات الصحية على مستوى إمارة دبي

https://nabidh.ae/#/comm/policies

ج. تُرسل طلبات الموافقة إلى البريد الإلكتروني: HISH@dha.gov.ae

4.15.2. إتخاذ كافة التدابير والضوابط والاشتراطات بشأن حماية خصوصية وسرية البيانات والمعلومات الصحية المنقولة ولتفادي مخاطر الكشف العرضي أو فقدان المعلومات إثناء النقل.

4.15.3. يجب تشفير المعلومات الصحية بشكل آمن أثناء عملية النقل، كما يجب التقيد بالضوابط والاشتراطات التي تم ذكرها في بنود هذه السياسة.

**4.16. التخلص من أصول المعلومات الصحية المحمية**

4.16.1. يتوجب على المنشأة الإلتزام بكافة القوانين والتشريعات القانونية لجميع المعلومات الصحية المؤرشفة أو التي تم التخلص منها، حسب القانون الاتحادي رقم (2) لسنة 2019 في شأن استخدام تقنية المعلومات والاتصالات في المجالات الصحية وسياسات الهيئة والتي تحتوي على الإرشادات التفصيلية حول الحد الأدنى لفترات الاحتفاظ بالمعلومات الصحية وإجراءات التخلص منها.

4.16.2. يقع على عاتق المنشأة التزام قانوني بالحفاظ على معايير السرية لجميع عمليات الأرشفة والتخلص من المعلومات الصحية.

4.16.3. يتم التخلص من الأجهزة الإلكترونية التي قد تحتوي على معلومات صحية (أجهزة الكمبيوتر، وأجهزة الكمبيوتر المحمولة، وأي أجهزة أخرى ذات قدرات تخزين المعلومات) بطريقة تضمن إزالة جميع البيانات بشكل فعال قبل إتلافها.

**4.17.خرق وانتهاك خصوصية وسرية المعلومات الصحية:**

4.17.1. عملية خرق لأمن المعلومات وانتهاك خصوصيتها وسريتها بشكل قد يؤدي إلى تلف عرضي أو غير قانوني للمعلومات الصحية، ضياعها، تغييرها، استخدامها، نسخها، طمسها، غلقها، محوها، إخفائها، أو الكشف والإفصاح عنها دون تصريح، أو الوصول إلى المعلومات الصحية ا المنقولة، تخزينها أو معالجتها بطريقة غير مناسبة، والتي تقع تحت طائلة المحاسبة وضمن سوء السلوك المهني (وهي على سبيل المثال لا الحصر):

أ. الإفصاح غير القانوني عن المعلومات الصحية المحمية.

ب. الوصول غير مصرح به للمعلومات الصحية المحمية، وحيث لا يوجد دواع إكلينيكية أو طبية له.

ج. الاستخدام غير المبرر/ إساءة استخدام المعلومات الصحية المحمية.

د. فقدان المعلومات الصحية المحمية.

هـ. الإفصاح الغير المصرح له أو النسخ للمعلومات الصحية المحمية.

و. الوصول إلى المعلومات الصحية المحمية من قبل طرف ثالث غير مصرح له.

ز. إجراء متعمد أو عرضي (أو تقاعس) من قبل المتحكم أو المعالج.

ح. إرسال المعلومات الصحية المحمية لجهة خطأ.

ط. فقدان أو سرقة أجهزة الكمبيوتر التي تحتوي على المعلومات الصحية المحمية.

ي. تعديل أو تغيير في المعلومات الصحية المحمية دون الحصول على الموافقة.

ك. إعادة تحديد الهوية للمعلومات الصحية المحمية مجهولة الهوية دون موافقة صاحب البيانات.

4.17.2. يُعد خرق وانتهاك الخصوصية أو الإفصاح غير المصرح به عن المعلومات الصحية المحمية إجراء غير قانوني يخضع للمساءلة واتخاذ الإجراءات التأديبية بشأنه.

4.17.3. قد ينتج عن أي انتهاك أو خرق لخصوصية وسرية المعلومات الصحية المحمية أثار وخيمة على القطاع الصحي وأصحاب البيانات وكذلك الموظفين العاملين في المجال. وعليه يتوجب على المنشأة الصحية (بصفتها المتحكم في المعلومات الصحية) والشخص المعالج للمعلومات الصحية المحمية الالتزام الكامل بكافة القوانين والتشريعات السارية في الدولة وكذلك اللوائح التنظيمية المعتمدة من قبل الهيئة بهذا الشأن.

**4.18. الإبلاغ عن انتهاك خصوصية وسرية المعلومات الصحية المحمية**

4.18.1. تلتزم المنشآت بإيجاد آلية الإبلاغ وإدارة حالات الانتهاك لخصوصية وسرية المعلومات الصحية المحمية (الإبلاغ عن الحادثة واستمرارية الأعمال)، وكذلك (خطة التعافي وإدارة الأزمات) والتي تتكون من: -

أ. تحديد نوع الانتهاك أو خرق الخصوصية

ب. السبب الرئيس لحدوث الخرق (جذور المشكلة)

ج. أنماط الحادث (متكرر أو جديد)

د. الخدمات المتأثرة بالحادث

هـ. إجراءات الاحتواء/ القضاء/ إزالة هذا الحادث

و. خطة التعافي واستعادة المعلومات الصحية

ز. الإجراءات / الخطط التحسينية والوقائية

ح. توثيق الدروس المستفادة من الحدث

4.18.2. إجراء تحقيق دقيق لتحري أسباب حدوث هذه الانتهاك / الحوادث وذلك بدءاً من نقطة اكتشاف الحادث وحتى الأغلاق، مع تحديد النقاط الآتية:

أ. تحديد طبيعة الاختراق أو الانتهاك ومدى علاقته بالمعلومات الصحية المحمية

ب. تحديد إذا كانت هناك حاجة لمزيد من التحقيقات، وفي حال عدم الحاجة، يتم توثيق الحادث والاحتفاظ بهذا السجل

ج. إجراءات التخفيف، خطة التعافي والعقوبات

4.18.3. يجب أن يكون التحقيق في حالة الانتهاك والتوثيق متضمناً الآتي:

أ. منظماً / مرتباً وموثقاً وفقاً للوائح التنظيمية المعتمدة بهذا الشأن

ب. استخدام إجراءات التحقيق المناسبة مع الاحتفاظ بتسلسل الأحداث

ج. إشراك الأفراد المدربين على التعامل مع مثل هذه الحوادث، عند الحاجة

د. التوعية والتوثيق لسبب وكيفية منع تكرار مثل هذه الأحداث

4.18.4. على المنشأة الإبلاغ عن الاختراقات / حوادث الانتهاكات ضمن الفترة الزمنية التي تم تحديدها وفقاً للائحة التنفيذية للقانون الاتحادي رقم (45) لسنة 2021 في شأن حماية البيانات الشخصية.

4.18.5. يتم إبلاغ كلاً من مكتب الإمارات للبيانات وكذلك الهيئة عبر البريد الإلكتروني التالي: HISH@dha.gov.ae

4.18.6. يجب أن يتضمن التقرير الاتي:

أ. بيان طبيعة الاختراق أو الانتهاك

ب. تاريخ الاختراق

ج. كيفية اكتشاف الاختراق

د. أسباب الاختراق أو الانتهاك

هـ. الفئات والعدد التقريبي للمعلومات وسجلاتها

و. مدى خطورة / جسامة الاختراق والآثار المحتملة

ز. الإجراءات الرسمية المتخذة من قبل المنشأة و/أو معالج المعلومات الصحية للإبلاغ عن الانتهاكات والتحقيق فيها وتسجيلها

ح. الإجراءات التصحيحية المتخذة من قبل المنشأة و/ أو معالج المعلومات الصحية

ط. المعلومات عن مسؤول حماية البيانات في المنشأة

4.18.7. على معالج المعلومات الصحية إبلاغ المنشأة فوراً في حال تحديد إي خرق أو انتهاك في البيانات والمعلومات الصحية المحمية

4.18.8. على المنشأة التي ترغب في الإبلاغ عن الحوادث المتعلقة بحماية المعلومات الصحية وخصوصيتها إتباع إجراءات الإبلاغ عن الحوادث وكما وردت في سياسة إدارة الحوادث المطبقة من قبلها.

4.18.9. أن يخضع الموظفين المخالفين لهذه السياسة إلى إجراءات تأديبية قد تمتد إلى إنهاء الخدمة

4.18.10. في حال كان الانتهاك أو الاختراق من شأنه تعرض خصوصية وسلامة المعلومات الصحية إلى مخاطر كبيرة فأنه يجب إبلاغ صاحب البيانات بهذا الانتهاك خلال الفترة الزمنية التي تحددها اللائحة التنفيذية للقانون الاتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية في الدولة.

4.18.11. يجب أن يكون بلاغ صاحب البيانات واضحاً وبلغة بسيطة مفهومة / متضمناً الاتي:

أ. طبيعة الاختراق أو الانتهاك المعلومات الصحية

ب. الآثار المحتملة لهذا الاختراق

ج. مدى تأثير هذا الاختراق على خصوصية صاحب البيانات وسرية المعلومات الصحية

د. أسم وتفاصيل التواصل مع مسؤول حماية البيانات بالمنشأة

هـ. الإجراءات المتخذة / أو المقترحة لمعالجة هذا الاختراق

4.18.12. يعتبر مسؤول حماية البيانات في المنشأة هو نقطة التواصل الأساسية لجميع حوادث الاختراق أو الانتهاك

4.18.13. طلب المشورة والنصح في أسرع وقت ممكن عن طريق التواصل مع الهيئة عبر البريد الإلكتروني: HISH@dha.gov.ae.

**4.19. تعيين مسؤول حماية البيانات والمعلومات الصحية:**

4.19.1 وفقاً لما نص عليه القانون الاتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية، فإنه يتوجب على كلا من المنشآت الصحية ومعالجين البيانات والمعلومات الصحية تعيين مسؤول لحماية البيانات والمعلومات الصحية، تتوفر فيه المهارات المهنية والدراية الكافية في مجال حماية البيانات، وذلك لاتخاذ الإجراءات المناسبة في أي من الأحوال الآتية:

أ. إذا تضمنت المعالجة مخاطر كبيرة بشأن مستوى سرية وخصوصية البيانات

والمعلومات الصحية نتيجة استخدام تقنيات جديدة أو مرتبطة بحجم البيانات.

ب. إذا احتوت المعالجة على تقييم ممنهج وشامل للبيانات والمعلومات الصحية بما يشمل التنميط والمعالجة المؤتمتة.

ج. إذا كانت المعالجة ستتم على حجم كبير من المعلومات الصحية.

4.19.2 يجوز أن يكون مسؤول حماية البيانات موظفاً لدى المنشأة (بصفتها المتحكم في البيانات والمعلومات الصحية) و / أو معالج البيانات والمعلومات الصحية أو كطرف خارجي من داخل أو خارج الدولة

4.19.3 يجب على المنشأة (بصفتها المتحكم في البيانات والمعلومات الصحية) و/ أو معالج البيانات والمعلومات الصحية في تحديد عناوين التواصل مع مسؤول حماية البيانات وإخطار مكتب الإمارات للبيانات والهيئة بالتفاصيل

**4.20. مهام وواجبات مسؤول حماية البيانات والمعلومات الصحية**

4.20.1. يعتبر دور مسؤول حماية البيانات والمعلومات الصحية دور رئيس لضمان امتثال المنشأة (بصفتها المتحكم في البيانات والمعلومات الصحية) وكذلك معالج البيانات لكافة القوانين والتشريعات السارية بشأن حماية البيانات والمعلومات الصحية، وكذلك اللوائح التنظيمية الصادرة عن الهيئة.

4.20.2. يتولى مسؤول حماية البيانات والمعلومات الصحية المهام والصلاحيات الآتية:

أ. التحقق من تطبيق كافة التدابير والإجراءات المعمول بها بشأن حماية وسلامة البيانات

والمعلومات الصحية وضمان الامتثال للقوانين والتشريعات السارية بشأن حماية البيانات ووفقاً لإرشادات هذه الوثيقة.

ب. ضمان دقة وصحة الإجراءات المتبعة من قبل كلا من المنشأة (المتحكم) والمعالج.

ج. تلقي كافة الشكاوى المتعلقة بأمن وسلامة البيانات والمعلومات الصحية.

د. تقديم النصح والاستشارات التقنية المرتبطة بالتقييم والفحص الدوري لأنظمة حماية البيانات والمعلومات الصحية، أنظمة منع الاختراق لدى كل من المنشأة (المتحكم) والمعالج.

هـ. توثيق نتائج التقييمات وإجراءات تقييم المخاطر

و. توفير قنوات تواصل مباشر مع الإدارة العليا والمدير التنفيذي

ز. تقديم النصح والمشورة اللازمة للموظفين، موردين الخدمة والاستشاريين والشركاء المرتبطين بإجراءات حماية البيانات والمعلومات الصحية.

ص. التوعية بالقوانين والتشريعات السارية في الدولة بشأن حماية البيانات والمعلومات الصحية وكذلك اللوائح التنظيمية المتبعة من قبل الهيئة، بما في ذلك تطوير السياسات والإجراءات الداخلية لإرشاد موظفي المنشأة ذوي العلاقة ومزودي الخدمة والاستشاريين وشركاء المنظومة بالإجراءات والعمليات التي من شأنها تعزيز امن وسلامة البيانات والمعلومات الصحية.

ر. على مسؤول حماية البيانات الالتزام بالحفاظ على سرية البيانات والمعلومات الصحية

التي يتلقاها لتنفيذ مهامه.

**4.21. التزامات المنشآت الصحية (المتحكم):**

4.21.1. تطوير سياسة داخلية ووضع التدابير اللازمة لحماية البيانات والمعلومات الصحية وخصوصيتها وضمان التعامل مع جميع المعلومات الصحية التي تم الحصول عليها، وحفظها، وتسجيلها، واستخدامها، وتخزينها، والتخلص منها بطريقة آمنة وسرية، وضمن مبادئ حماية البيانات والمعلومات الصحية التي نصت عليها القوانين الاتحادية في الدولة والتشريعات السارية بإمارة دبي، واللوائح التنظيمية للهيئة.

4.21.2. توفير ضمانات إدارية وتقنية ومادية مناسبة للمراقبة، التدقيق وحماية البيانات والمعلومات الصحية والتحقق من حماية البيانات والمعلومات الصحية التي يتم التعامل معها ضمن المنشأة وبما يتماشى مع الشروط والضوابط المحددة في هذه السياسة.

4.21.3. القيام بتقييم حماية البيانات والمعلومات الصحية على أساس سنوي وكذلك أثناء التعامل مع مبادرة / مشروع جديد من المحتمل أن يؤدي إلى مخاطر عالية على المعلومات الصحية المحمية، ويمكن العثور على إرشادات إجراء التقييم من خلال الرابط الآتي: https://gdpr.eu/data-protection-impact-assessment-template/

4.21.4. إجراء تدقيق متعلق بمدى الامتثال لتقييم فعالية تطبيق تدابير الحماية على المعلومات الصحية وتحديد/ تخفيف المخاطر المحتملة.

4.21.5. تطبيق العقوبات المناسبة تجاه الموظفين، المتدربين، مزودي الخدمة والمتعاقدين الخارجين والتي ثبت مخالفتهم أو وجود خرق للسياسات والإجراءات المتخذة لحماية

البيانات الصحية.

4.21.6. ضمان اقتصار الوصول إلى المعلومات الصحية على المصرح لهم فقط ولديهم صلاحية محددة الغرض لمراجعة و/ أو تغيير البيانات، وذلك بالتحقق من وجود الإجراءات والتدابير اللازمة للتخصيص والتحكم في الوصول إلى المعلومات وكذلك رمز الدخول.

4.21.7. التأكد من التسجيل:

أ. جميع التطبيقات وقواعد البيانات المستخدمة للتعامل مع المعلومات الصحية في المنشأة.

ب. أغراض الاحتفاظ بالبيانات الصحية داخل هذه التطبيقات

ج. آلية استخدام المعلومات الصحية وتحديد الأشخاص المصرح لهم بالوصول إليها.

4.21.8. تطوير سياسة داخلية لـ " أمن المعلومات" مع مراعاة الأحكام والضوابط ذات الصلة بقوانين الدولة وإمارة دبي، هذه السياسة وجميع اللوائح التنظيمية المعتمدة من قبل الهيئة بشأن حماية أصول المعلومات الصحية.

4.21.9. ضمان التزام مستخدمي المعلومات بالسياسات والإرشادات الصادرة بشأن إدارة أصول المعلومات الصحية.

4.21.10. على مزودي خدمات منصات الصحة الرقمية التأكد من تطبيق شرط إشعار أصحاب البيانات بمعالجة معلوماتهم الصحية.

أ. ويجب أن تتضمن إشعارات صاحب البيانات الآتي:

1.أ. طبيعة ونوع المعلومات الصحية المحفوظة

2.أ. السبب في الاحتفاظ بهذه المعلومات الصحية

3.أ. كيفية استخدام هذه المعلومات

4.أ. الجهة التي سيتم الإفصاح لها عن المعلومات الصحية

ب. يتم تقديم إشعار معالجة المعلومات الصحية إلى صاحب البيانات عبر استخدام الإشعار الورقي و/ أو الموقع الإلكتروني لمزود الخدمة.

ج. أن يوضح إشعار المعالجة لصاحب البيانات كيفية ممارسة حقوقهم القانونية بشأن بياناتهم ومعلوماتهم الصحية، وكذلك تزويدهم برابط الكتروني لكافة التشريعات والقوانين واللوائح التنظيمية الخاصة بحماية البيانات والمعلومات الصحية كاملاً.

4.21.11. الإمتثال لجميع قوانين الدولة وكذلك التشريعات السارية في إمارة دبي والشروط والضوابط المتبعة من قبل الهيئة بشأن تنظيم الصحة الرقمية، التطبب عن بعد، تبادل المعلومات الصحية الرقمية، حماية البيانات، جودة البيانات، سرية وخصوصية البيانات، الشفافية، الأمن السيبراني وأمن المعلومات.

4.21.12. الإمتثال لجميع التشريعات السارية في الدولة بشكل عام وإمارة دبي والهيئة بشكل خاص فيما يتعلق بحماية البيانات والمعلومات الصحية.

4.21.13. الامتثال للقواعد والمبادئ المتبعة من قبل مركز دبي للأمن الإلكتروني (DESC) ولوائح هيئة تنظيم الاتصالات والحكومة الرقمية (TDRA) في الدولة.

4.21.14. مراعاة تدابير أمن المعلومات:

أ. قرار المجلس التنفيذي رقم (13) لسنة 2012 بشأن تنظيم أمن المعلومات في حكومة دبي

ب. تنظيمات حماية وأمن المعلومات والبيانات ISR

ج. مركز دبي للأمن الإلكتروني

هـ. هيئة دبي الرقمية

و. الهيئة الوطنية للأمن الإلكتروني في الدولة NESA

ز. تطبيق مقاييس ISO 27001 لإدارة أمن المعلومات

4.21.15. الامتثال للتشريعات الاتحادية والمحلية، بما فيها على سبيل المثال لا الحصر:

أ. المرسوم بقانون اتحادي رقم (4) لسنة 2016 بشأن المسؤولية الطبية، ولائحته التنفيذية، والقرارات الصادرة بموجبها.

ب. القانون رقم (26) لسنة 2015 بشأن تنظيم نشر وتبادل البيانات في إمارة دبي

ج. معايير وإرشادات الأمن الإلكتروني الفيدرالية للدولة وسلطة الأمن الإلكتروني لإمارة دبي للأمن السيبراني

4.21.16. الامتثال لجميع السياسات المطبقة من قبل الهيئة بشأن:

أ. سياسات ومعايير نظام "نابض"

ب. سياسة تصنيف أصول البيانات والمعلومات في المجالات الصحية على مستوى إمارة دبي

ج. سياسة جودة البيانات والمعلومات الصحية

ه. سياسة أمن المعلومات الصحية

4.21.17. وضع التدابير المناسبة لتقييم وتحديد مستوي الامتثال والفعالية لنظام إدارة أمن المعلومات(ISMS) من قبل المنشاة.

4.21.18. مراجعة التغيير في التطبيقات والمشاريع الإلكترونية من منظور أمن المعلومات.

**4.22. المهام والمسؤوليات ضمن المنشأة: -**

4.22.1. على المنشأة تطبيق ضوابط حماية البيانات والمعلومات الصحية، والتقيد بالتشريعات السارية في دولة الإمارات العربية المتحدة وإمارة دبي والهيئة.

4.22.2. أن يكون الأشخاص المصرح لهم الوصول إلى المعلومات الصحية داخل المنشأة على دراية بمسؤولياتهم والتزاماتهم.

4.22.3. أدناه، الجدول المُوجّز للأدوار والمسؤوليات داخل المنشأة:

| الأدوار والمسؤوليات |
|---|

| | |
|---|---|
| **المدير التنفيذي** | • يتحمل الرئيس التنفيذي المسؤولية النهائية لضمان اتخاذ المنشأة الإجراءات والتدابير والتنظيمية الملائمة لإدارة حماية البيانات وخصوصيتها.<br>• التحقق من وجود الضمانات الكافية التي تدعم سياسات المنشأة في تنفيذ واستخدام ومعالجة المعلومات الصحية وأن المعالجة تتم بشفافية وضمن إجراءات وتدابير ملائمة وفق القوانين والتشريعات السارية بهذا الشأن.<br>• ضمان توفير الموارد الكافية لتلبية متطلبات السياسة في المنشأة ودور مسؤول حماية البيانات. |
| **مسؤول حماية البيانات والمعلومات الصحية** | • تم توضيح مهام ومسؤوليات مسؤول حماية البيانات والمعلومات الصحية في بنود السياسة |
| **المدراء المباشرين** | **على المدراء المباشرين التحقق من إن الموظفين الدائمين والمؤقتين ومزودي الخدمة على دراية بما يلي: -**<br>• سياسة حماية امن وسلامة البيانات والمعلومات الصحية من حيث صلتها بمجالات عملهم.<br>• المسؤولية الشخصية في التعامل مع المعلومات الصحية.<br>• الامتثال لمتطلبات إعداد التقارير.<br>• آلية الحصول على المشورة بشأن التعامل مع المعلومات الصحية.<br>• التأكد من تلقي الموظفين المعنيين التدريب المطلوب.<br>• المسؤولية بشكل مباشر في الحفاظ على الامتثال لحماية البيانات والمعلومات الصحية داخل الإدارات التابعة لهم / مجال المسؤولية. |
| **الموظفين** | وفقا للقانون الاتحادي رقم 45 لسنة 2021 بشأن حماية البيانات الشخصية:<br>• تلتزم المنشاة بالحفاظ على البيانات الخاصة بالموظفين المعينين لديها وحماية خصوصيتها.<br>• التزامات موظفي المنشأة ومقدمي الرعاية الصحية تجاه صاحب البيانات والمعلومات الصحية وفقاً للتشريعات والقوانين السارية بهذا الشأن<br>كما يتوجب على جميع الموظفين:<br>• التقيد بالتشريعات القانونية بشأن الحفاظ على سرية المعلومات الصحية، ضمان عدم مخالفة مبادئ حماية البيانات والحفاظ على حقوق صاحب البيانات. |

| | |
|---|---|
| | • المشاركة في الدورات التدريبية التعريفية والتوعوية.<br>• أن يكون الموظفين على معرفة بمسؤولي حماية البيانات والمعلومات الصحية في المنشأة ومهامهم.<br>• التحقق عند الحاجة من هوية أي شخص يتقدم بطلب للحصول على معلومات سرية وتحديد صحة سبب طلب تلك المعلومات.<br>• الإبلاغ مباشرة عن حوادث الخرق أو الانتهاكات الفعلية أو المشتبه بها لسرية المعلومات إلى المدير المباشر. |

**4.23. التدريب**

4.23.1. على المنشأة ضمان توفير خطط التدريب والتوعية المناسبة لدعم الإمتثال لهذه السياسة.

4.23.2. يعتبر التدريب على أمن وحماية البيانات أمرًا إلزاميًا ويجب توفيره للموظفين عند بداية التوظيف وتكراره كل عامين للتأكد من أنهم على دراية بالشروط والضوابط الخاصة في التعامل مع المعلومات الصحية وبما يتماشى مع هذه السياسة.

4.23.3. يتوجب على المنشآت تدريب جميع الأفراد المتعاملين معها مثال: الموظفين والمتدربين ومزودي الخدمة، الشركات المتعاقدة معها وأي شخص أخر مرتبط بمعاملة البيانات والمعلومات الصحية في المنشأة، على سياسات وإجراءات الخصوصية الخاصة بها، ووفقاً لما تقتضيه الضرورة والملاءمة لأداء مهامها.

4.23.4. يجب أن يكون لدى المنشأة عملية مراجعة وتقييم دورية لكفاءة الموظفين والموارد الأخرى بما في ذلك موردي الخدمة.

4.23.5. يجب على الجهة مراجعة الدورات التدريبية والتوعوية بشكل دوري لتعكس قوانين الدولة الحالية والمتطلبات التنظيمية للهيئة.

**4.24. المساءلة**

4.24.1. تعتبر المنشأة مسؤولة بشكل كامل عن الامتثال لجميع قوانين دولة الإمارات العربية والتشريعات السارية في إمارة دبي وكافة الأنظمة واللوائح السارية في الهيئة، ويجب إثبات هذا الالتزام.

4.24.2. تلتزم المنشأة قانونياً باتخاذ التدابير والإجراءات المناسبة للحفاظ على سرية وخصوصية البيانات والمعلومات الصحية لديها.

4.24.3. يتعين على المنشآت اجراء عمليات تدقيق داخلية وخارجية دورية ومراجعات مستقلة لمراقبة الامتثال لمتطلبات حماية البيانات والمعلومات الصحية على النحو المحدد في هذه السياسة.

4.24.4. يتعين على المنشآت الصحية تقديم نتائج التدقيق / الامتثال للهيئة بشكل سنوي

**4.25. عدم الإمتثال:**

4.25.1. يعتبر عدم الالتزام بإرشادات هذه الوثيقة مخالفة تستوجب اتخاذ الإجراءات التأديبية وفق أحكام التشريعات السارية.

**في حال التباين والاختلاف أو التعارض بين النسخة العربية والنسخة الإنجليزية، يعتد بالنسخة العربية.**

## 5. References

5.1. Federal Law No. (2) of 2019, Concerning the Use of the Information and Communication Technology in the Area of Health ("ICT Health Law"). Available on: https://mohap.gov.ae/app_content/legislations/php-law-ar-95/mobile/index.html#p=1

5.2. Cabinet Decision No. (32) of year 2020 on the Implementing Regulation of UAE Federal Law No. (2) of year 2019 on the Use of Information and Communication Technology in Health Fields. Available on:

https://mohap.gov.ae/app_content/legislations/php-law-ar-95/mobile/index.html#p=1

5.3. Cabinet Decision no. (51) of 2021 on exemption for storage and transfer of health data and information outside the country. Available on:

https://mohap.gov.ae/app_content/legislations/php-law-ar-120/mobile/index.html

5.4. Federal Decree-Law No. (45) of 2021 on the Protection of Personal Data (United Arab Emirates). Available on:

https://u.ae/ar-ae/about-the-uae/digital-uae/data/data-protection-laws#personal-data-protection-law

5.5. DHA_HISHD Health Information Assets Classification Policy. Available on:

https://nabidh.ae/#/comm/policies.

5.6. Resolution No. (2) of 2017 Approving the Policies Document on Classification, Dissemination, Exchange, and Protection of Data in the Emirate of Dubai. Available on: https://www.smartdubai.ae/docs/default-source/dubai-data/dubai-data-policies-en.pdf?sfvrsn=b2019ec4_6#:~:text=Article%20(1),Emirate%20of%20Dubai%2C%20is%20approved.

5.7. Law No. (26) Of 2015 Regulating Data Dissemination and Exchange in the Emirate of Dubai. Available on:

https://www.smartdubai.ae/docs/default-source/dubai-data/data-dissemination-and-exchange-in-the-emirate-of-dubai-law_2015.pdf?sfvrsn=46ac2296_6.

5.8. The Telecommunications and Digital Government Regulatory Authority (TDRA) of the United Arab Emirates (UAE). Available on:

https://www.tdra.gov.ae/en/about-tra/about-tra-vision-mission-and-values.aspx

5.9. Federal Law No. (5) of year 2012 on Combatting Cybercrimes and its amendment by Federal Law No. (12) of 2016. Available on:

https://u.ae/ar-ae/resources/laws

5.10. Cabinet Resolution No. (24) of year 2020 On the Dissemination and Exchange of Health Information Related to Communicable Diseases and Epidemics and Misinformation Related to Human Health. Available on:

https://mohap.gov.ae/app_content/legislations/php-law-ar-91/mobile/index.html

5.11. Federal Decree Law No. (4) of year 2016 on Medical Liability. Available on: Medical Liability Law

5.12. Executive Council Resolution No. (32) of year 2012 on Regulating the Entity of health professions in the Emirate of Dubai. Available on:

Regulating the Entity of health professions in the Emirate of Dubai

5.13. Law No. (13) of 2021 establishing the Dubai Academic Health Corporation, and Law No. (14) of 2021 amending some clauses of Law No. (6) of 2018 pertaining to the Dubai Health Authority (DHA). Available on :

https://www.wam.ae/en/details/_1395302953555

5.14. Dubai Health Authority Nabidh policies and standards. Available on: https://nabidh.ae/#/comm/policies

5.15. Dubai Health Authority Policy for Use of Artificial Intelligence in the Healthcare in the

Emirate of Dubai. Available on: https://nabidh.ae/#/comm/policies

5.16. Dubai Health Authority Code of Ethics and Professional Conduct (2014). Available on: DHA Code of Conduct

5.17. Dubai Government Information Security Regulation (ISR). Available on: https://www.desc.gov.ae/regulations/standards-policies/

5.18. UAE National Electronic Security Authority (NESA). Available on: https://logrhythm.com/solutions/compliance/uae-national-electronic-security-authority/

5.19. Requirements for an Information Security Management System (ISMS), ISO 270001. Available on:

https://www.iso.org/isoiec-27001-information-security.html

5.20. The General Data Protection Regulation (GDPR) (from Must 2018). Available on: https://gdpr-info.eu/art-84-gdpr/

5.21. DOH Standard-on-Patient-Healthcare-Data-Privacy. Available on :

https://www.doh.gov.ae/-/media/Feature/Aamen/DOH-Standard-on-Patient-Healthcare-Data-Privacy.ashx

5.22. A pilot comparison of medical records sensitivity perspectives of patients with must behavioral health conditions and healthcare providers. Hiral Soni, Julia Ivanova, Adela Grando, Anita Murcko 1, Darwyn Chern, Christy Dye 2, Mary Jo Whitfield 3 Health Informatics J. Apr-Jun 2021; 27(2): 14604582211009925. Available on : https://doi.org/10.1177/14604582211009925

5.23. UK Iinformation Commissioner's Office website. Available on: www.ico.org.uk.