نوع الوثيقة: سياسة المعلومات الصحية	**الرمز الكودي:** DHA/HISHD/PP-13	**رقم الإصدار: 1**
عنوان السياسة: سياسة مشاركة البيانات والمعلومات الصحية	**تاريخ الإصدار:** 2024 /08/10 **تاريخ التفعيل:** 2024 /11/10 **تاريخ المراجعة:** 2029 /08/10	
ملكية الوثيقة: هيئة الصحة في دبي		
نطاق التطبيق: المنشآت الصحية العاملة ضمن نطاق اختصاص وصلاحيات هيئة الصحة في دبي		

1. التعاريف:

في تطبيق أحكام هذه السياسة، يقصد بالكلمات والعبارات التالية المعاني المبينة قرين كل منها ما لم يدل سياق النص بغير ذلك.

الدولة: دولة الإمارات العربية المتحدة

الإمارة: إمارة دبي

الهيئة: هيئة الصحة في دبي

المنشأة: أي جهة أو مؤسسة صحية داخل الإمارة تقدم خدمات صحية للأشخاص، وتشمل: مجالات الوقاية والعلاج والنقاهة، سواء كان من يملكها أو يتولى إدارتها شخص طبيعي أو اعتباري، كما يمكن أن تشمل مقدمي خدمات تأمين صحي أو ضمان صحي أو التوسط فيه أو إدارة متطلباته أو خدمات الكترونية في المجال الصحي، أو أية خدمات ترتبط بشكل مباشر أو غير مباشر بتطبيق أحكام هذه السياسة.

الإمتثال: الالتزام والتقيد بالتشريعات السارية والقرارات الصادرة بموجبها من السلطة المختصة.

السرية: حماية البيانات والمعلومات من الاطلاع عليها أو تداولها من قبل غير المخولين بذلك وفق التشريعات السارية بهذا الشأن.

الموافقة: تصريح من صاحب البيانات للغير بالاطلاع أو معالجة بياناته الشخصية. وتكون الموافقة محددة وواضحة بشكل لا لبس فيه.

المتحكم: هي الجهة التي لديها البيانات والمعلومات الصحية وبحكم النشاط تقوم بتحديد طريقة وأسلوب ومعايير معالجة هذه البيانات والمعلومات والغاية من معالجتها. في هذه السياسة المتحكم في البيانات الصحية هي المنشأة.

البيانات: مجموعة منظمة من المعلومات أو الحقائق أو المفاهيم أو التعليمات أو الملاحظات أو القياسات على شكل أرقام أو حروف أو كلمات أو رموز أو صور أو مقاطع فيديو أو إشارات أو أصوات أو خرائط أو أي شكل آخر، يتم إنشاؤها أو معالجتها أو تخزينها أو تفسيرها أو يتم تبادلها من قبل الأفراد أو تكنولوجيا المعلومات والاتصالات (ICT).

المعلومات الصحية: البيانات الصحية التي تمت معالجتها وأصبحت لها دلالة سواء كانت مرئية أو صوتية أو مقروءة، والتي تتسم بالصبغة الصحية سواءً تعلقت بالمنشآت أو الجهات الصحية أو التأمينية أو المستفيدين من الخدمات الصحية.

إخفاء الهوية: تقنية لمعالجة البيانات تُزيل أو تُعدّل معلومات تحديد الهوية الشخصية، فتسفر هذه التقنية عن بيانات مخفية الهوية لا يمكن نسبتها لأي فرد من الأفراد لمعلومات مخفية الهوية ليست قادرة على تحديد هوية الفرد؛ ولا يمكن استخدامها عمليا لتحديد هويتهم. يتطلب إخفاء الهوية إزالة أي معرف مباشر وأشباه معرفات (مثل التفاصيل، أو مجموعة من التفاصيل، التي قد تتيح تحديد الهوية، إما بمفردها أو عند استخدامها مع المعلومات الأخرى المتاحة). المعلومات المجهولة الهوية بشكل فعال (حيث يكون احتمال تحديد هوية الأفراد مستبعداً)، لا يُنظر إليها على أنها بيانات شخصية، وبالتالي لا تنطبق عليها قوانين حماية البيانات. يمكن استخدام المعلومات مخفية الهوية أو الكشف عنها دون موافقة صاحب البيانات/ المريض،

بحيث لا تحدد هذه المعلومات هوية صاحب البيانات ومع ذلك، يجب أن يتم إخفاء الهوية بشكل فعال، ولا يجب أن يكون لعملية إخفاء الهوية، ولا استخدام المعلومات مخفية الهوية، أي تأثير ضار مباشر على أي فرد معين.

اتفاقية مشاركة البيانات: اتفاقية رسمية موقعة بين المنشاة (كمتحكم) ومقدم الطلب (كمعالج) للموافقة على مشاركة البيانات وفقاً لشروط وأحكام محددة ومتوافقة مع مبادئ مشاركة البيانات.

تقييم حماية البيانات: تقييم المخاطر المحتملة على خصوصية وسرية البيانات الصحية والإجراءات والتدابير المقترحة للحد من المخاطر المحتملة على حماية البيانات الصحية، وكيفية تقليل أو تفادي هذه المخاطر في مرحلة مبكرة من المعالجة وإلى أقصى حد ممكن.

أصول البيانات والمعلومات ومنها:

- نسخ إلكترونية من البيانات والمعلومات الصحية
- نسخ مطبوعة من البيانات والمعلومات الصحية
- تطبيقات برمجية
- الأجهزة والمعدات التي تستخدمها المنشأة لمعالجة البيانات والمعلومات وتخزينها.
- كافة البيانات والمعلومات المتاحة في المنشأة أو متاحة للاستخدام من قبل الموارد البشرية.

الإفصاح عن البيانات: هو نقل أو مشاركة البيانات الصحية من المصرح له مع طرف آخر.

مشاركة المعلومات الصحية: الوصول إلى البيانات والمعلومات الصحية أو تبادلها أو نسخها أو تصويرها أو نقلها أو تخزينها أو نشرها أو الكشف عنها أو نقلها.

الطرف الآخر: الأشخاص الطبيعية أو الاعتبارية التي تتعامل مع المنشأة من خلال علاقة عمل أو تم التصريح لها بالوصول إلى أياً من البيانات أو المعلومات الصحية لهذه المنشأة.

الممارسة السريرية الجيدة: هي معيار جودة دولي لإجراء التجارب السريرية التي يتم توفيرها في بعض البلدان من خلال المؤتمر الدولي للتنسيق (ICH)، وهي هيئة دولية تحدد مجموعة من المعايير، والتي يمكن

للمؤسسات تحويلها إلى لوائح التجارب السريرية التي تشمل البشر.

مشاركة البيانات والمعلومات الصحية: الوصول إلى البيانات والمعلومات الصحية، تبادلها، نسخها وتصويرها ونقلها، تخزينها ونشرها والإفصاح عنها أو نقلها.

المعالجة: تشمل إنشاء البيانات وإدخالها واستخدامها وتعديلها وتحديثها وحذفها وتخزينها والإفصاح عنها والتخلص منها.

الحوادث: الحادث الأمني هو حدث يؤدي إلى انتهاك أو تهديد وشيك بانتهاك سياسات أمن المعلومات، أو سياسات الاستخدام المقبول، أو معيار الأمان المعلوماتي للمتحكم بالبيانات؛ ويعرض البيانات الحساسة لخطر التعرض.

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

المعلومات الصحية المحمية: تعني البيانات والمعلومات المتعلقة بشخص طبيعي يمكن تحديدها أو يمكن التعرف على صاحبها (صاحب البيانات)؛ بشكل مباشر أو غير مباشر، على وجه الخصوص بالرجوع إلى معرف. وقد تكون المعرفات الشخصية، على سبيل المثال، الاسم أو رقم تعريف أو بيانات موقع أو محددات هوية بوسائل إلكترونية أو عنصرا محددا أو أكثر من عناصر الهوية. ويشار إليها أيضًا باسم المعلومات الصحية الشخصية؛ هي أي بيانات يمكن استخدامها، بشكل مباشر أو غير مباشر لتحديد هوية شخص ما ("موضوع البيانات"). على وجه الخصوص بالرجوع إلى معرف. وقد تكون المعرفات الشخصية، على سبيل المثال، الاسم أو رقم تعريف أو بيانات موقع أو محددات هوية بوسائل إلكترونية أو عنصرا محددا يختص بالهوية الجسدية أو الفسيولوجية أو الجينية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية لذلك الفرد. وهي التي تتضمن أي من المعرّفات الثمان عشرة (18) التالية[1]:

[1] The HIPAA Privacy Rule

- 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 الطبي/ 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 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 البيانات الصحية المحمية نيابة عن المتحكم ويقوم بمعالجتها وفقاً لتوجيهه وتعليماته.

التسمية المستعارة: المعالجة التي يتم إجراؤها على المعلومات الصحية المحمية بطريقة تؤدي إلى عدم إمكانية ربط أو تنسيب هذه البيانات 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.

الاستخدام الثانوي (غير المباشر) للبيانات والمعلومات الصحية: استخدام البيانات 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.

التشفير: استخدام عملية حسابية لتحويل البيانات إلى شكل يكون فيه احتمال ضئيل لتعيين المعنى دون استخدام عملية حسابية. سيؤدي هذا إلى منع الوصول غير المصرح به/ استخدام البيانات والمعلومات.

الملف الطبي الإلكتروني (المعروف أيضًا باسم الملف الصحي الإلكتروني): هو عبارة عن مجموعة منهجية من البيانات والمعلومات الصحية الإلكترونية للفرد بتنسيق رقمي يتوافق مع معايير التشغيل البيني المعترف بها على مستوى الدولة ويتيح استخدام المعلومات ومشاركتها عبر الشبكات الآمنة.

السجل الصحي: هي مجموعة منتظمة من البيانات والمعلومات جمعت من ملف المريض حول أمراض وحالات صحية معينة.

القاصر: من لم يبلغ الثامنة عشرة من عمره.

المعلومات الصحية الحساسة: فئات خاصة من المعلومات الصحية الشخصية التي تتطلب قدرًا أكبر من الحماية والتبرير للاستخدام والمشاركة. هذه المعلومات قد حددت مسبقا ضمن سياسة تصنيف أصول البيانات الصحية، وتشمل على سبيل المثال لا الحصر:

- معلومات عن تعاطي المخدرات.
- معلومات عن تعاطي الكحول.
- معلومات عن الصحة الجنسية (بما في ذلك الأمراض المنقولة جنسياً وعدوى فيروس نقص المناعة البشرية).
- معلومات عن الصحة الإنجابية.
- الصحة النفسية/ الصحة السلوكية.
- البيانات والمعلومات الجينية والوراثية.
- حمل المراهقات.
- حماية الطفل والقضايا ذات الصلة.

الملف الطبي/ الصحي: النظام الذي يستخدم لتوثيق البيانات والمعلومات الصحية والشخصية والإدارية الخاصة بكل شخص يتلقى الرعاية الصحية في ملف خاص به ويتم ذلك بشكل مستدام ومتكامل وآمن بهدف تحقيق سلامة وجودة الرعاية الصحية وتسهيل استخدام تلك البيانات والمعلومات من قبل مقدمي الخدمات الصحية وتنظيم تبادلها وفقا للتشريعات المعمول بها في الدولة.

الوصي الشرعي: شخص يعينه القانون لإعطاء الموافقة بدلاً من صاحب البيانات غير الكفء بناءً على قوانين الدولة، عندما يكون المريض غير قادر على تقديم الموافقة بسبب مرض أو عدم كفاءة.

شبه المعرفات: هي متغيرات في مجموعة البيانات لا تحدد بشكل مباشر ولكن يمكن أن يعرفها مهاجم البيانات وتستخدم لإعادة تحديد هوية الفرد.

المعرفات المباشرة: أي بيانات يمكن استخدامها، بشكل مباشر أو غير مباشر لتحديد هوية شخص ما ("موضوع البيانات").

صاحب البيانات: الشخص الذي تتعلق به البيانات والمعلومات الصحية، هذا الشخص يمكن أن يكون المريض أو أي فرد سليم.

صاحب البيانات/ المريض غير الكفء: يشير إلى صاحب البيانات/المريض الذي إما يفتقر إلى الأهلية القانونية الكاملة (الصغير غير المميز/ الشخص الذي يعاني من إعاقة ذهنية أو العجز العقلي) أو شخص لديه القدرة الكاملة، ولكنه غير قادر على تقديم الموافقة (على سبيل المثال فاقد للوعي).

طبيب/طبيب أسنان مقيم: هو طبيب الطب البشري/ طب الأسنان مسجل في نظام شربان يشارك في برنامج الدراسات العليا للطب البشري/ طب الأسنان المعتمد في الدولة؛ تحت الإشراف المباشر أو غير المباشر لطبيب بشري/ طبيب أسنان مسجل.

طلب الوصول للبيانات: هو طلب كتابي بالوصول بيانات أو معلومات صحية محددة، والذي بموجب اعتماده يصرح لمقدم الطلب بحيث يكون صاحب تلك البيانات أو المعلومات الصحية أو ممثله القانوني بالحصول على سجلات المعلومات الشخصية التي تحتفظ بها المنشأة .

2. الغرض

2.1. تحديد شروط وضوابط الهيئة لمشاركة البيانات والمعلومات الصحية والمحمية، بما يتوافق مع التشريعات والقوانين السارية بالدولة. بهذا الشأن.

2.2. التأكد من أن كافة المنشآت العاملة ضمن نطاق اختصاص وصلاحيات الهيئة توفر بيئة آمنة لمشاركة البيانات والمعلومات الصحية؛ وعلى وجه التحديد التي يطلق عليها أيضًا "المعلومات

الصحية المحمية".

2.3. توفير إطار عمل للضوابط اللازمة لمشاركة المعلومات الصحية المحمية، والتأكد من استيفاء المعايير المطلوبة.

2.1. حوكمة الإجراءات والأنظمة المتبعة بشأن البيانات والمعلومات الصحية، بما يضمن حمايتها والمحافظة على خصوصية صاحب البيانات والمعلومات، وضمان سريتها وعدم تداولها من قبل غير المصرح له.

3. مجال التطبيق.

3.1. جميع المعلومات الصحية المحمية التي تتم مشاركتها من قبل المنشآت الصحية الخاضعة لسلطة الهيئة.

3.2. البيانات والمعلومات الصحية، بجميع أشكالها، كما هو معرف في القانون الاتحادي رقم (2) لسنة 2019 بشأن استخدام تقنية المعلومات والاتصالات في المجالات الصحية. ويشمل ذلك على سبيل المثال لا الحصر:

2.3.1. البيانات والمعلومات الطبية والسجلات الصحية - على سبيل المثال: سجل الولادة، والوفاة، والحوادث والطوارئ، والعمليات، وما إلى ذلك)

2.3.2. البيانات والمعلومات الغير الطبية (مثال الموارد البشرية، سجلات الشكاوى، ملفات المنشأة - السجلات الإدارية المتعلقة بالمهام التشغيلية للمنشأة... الخ).

2.3.3. أصول المختبرات (كتل البارافين والشرائح والصور الرقمية وما إلى ذلك) وتقارير اختبار المريض.

2.3.4. تقارير الأشعة السينية والتصوير والمخرجات والصور.

2.3.5. البيانات المُعرفة والغير قابلة للتعريف.

2.3.6. البيانات والمعلومات التي يمكن الوصول إليها للاستخدام الأساسي أو الثانوي (مثل السجلات التي تتعلق باستخدامات غير عن الرعاية الصحية للمريض؛ على سبيل المثال، السجلات المستخدمة لإدارة الخدمات الصحية والتخطيط الصحي والأبحاث والجودة وما إلى ذلك).

2.3.7. ميكروفيلم.

2.3.8. شرائط صوت وفيديو، وأشرطة كاسيت، وأقراص مضغوطة، إلخ.

2.3.9. البيانات الورقية أو الرقمية.

2.3.10. أنظمة سجل البيانات المُهيّكلة (الورقية والإلكترونية).

3.3. جميع المستخدمين الذين لديهم صلاحية الوصول إلى البيانات والمعلومات الصحية والمحمية ويستخدمونها في قطاع الرعاية الصحية في الإمارة ؛ بما في ذلك جميع الموظفين والمتدربين والطلاب والمقاولين والاستشاريين والموردين والبائعين والشركاء والعملاء والشركاء في تقديم الخدمة على نطاق أوسع وكلما اقتضت الحاجة ذلك.

4. بيان السياسة

4.1. تعد سياسة مشاركة البيانات والمعلومات الصحية جزءًا لا يتجزأ من نهج الهيئة في حوكمة البيانات والمعلومات الصحية، مما يستوجب معها الرجوع إلى السياسات والمعايير المعتمدة في الهيئة ذات الصلة سياسات حوكمة البيانات الصحية.

4.2. السياسة راعت ما نصت عليه التشريعات السارية في الدولة والإمارة بشأن البيانات والمعلومات الصحية، وآلية معالجتها وتداولها.

4.3. تجميع واستخدام ومشاركة المعلومات الصحية المحمية:

4.3.1. يجب أخذ موافقة صاحب البيانات/ المريض من أجل جمع ومشاركة ومعالجة البيانات

والمعلومات الصحية (سياسة تصنيف أصول البيانات الصحية) وذلك بما يتوافق مع التشريعات والقوانين واللوائح الصادرة في الدولة بهذا الشأن بشكل عام والصادر عن الهيئة بشكل خاص

4.3.2. يجب أن تكون الموافقة وفقًا لمتطلبات هيئة الصحة بدبي (سياسة الموافقة والتحكم في الوصول).

4.4. المشاركة المنهجية والمشاركة الخاصة للمعلومات الصحية المحمية

تغطي هذه السياسة كلاً من مشاركة البيانات والمعلومات الصحية المنهجية والمخصصة:

4.4.1. مشاركة البيانات والمعلومات بشكل منهجي/ روتيني:

أ. تتم مشاركة البيانات والمعلومات بين مجموعة من المنشآت لغرض محدد، وفق أحكام التشريعات السارية، حيث يحظر تداول أياَ من البيانات والمعلومات الصحية دون موافقة كتابية من المريض باستثناء الحالات المحددة قانوناً.

ب. يجب أن تكون المشاركة المنهجية للمعلومات بين المنشآت تحت حوكمة اتفاقية/عقد التي تحدد القواعد والعملية للوصول إلى المعلومات الصحية المحمية واستخدامها.

4.4.2. مشاركة المعلومات المخصصة:

أ. هو كشف لمرة واحدة عن المعلومات الصحية المحمية للمصرح له بموجب التشريعات السارية. في بعض الحالات، قد ينطوي ذلك على قرار بشأن مشاركة المعلومات الصحية المحمية في حالة الطوارئ (مثل طوارئ الصحة العامة)، وفق أحكام التشريعات السارية، حيث يحظر تداول أياَ من البيانات والمعلومات الصحية دون موافقة كتابية من المريض باستثناء الحالات المحددة قانوناً.

ب. يجب النظر بعناية في جميع قرارات مشاركة البيانات المخصصة من قبل فريق حوكمة البيانات في المنشأة وتوثيقها. يجب تقييم الطلبات بعناية حسب كل حالة واتخاذ القرار بناءً

على:

أولا. نوع البيانات والمعلومات الصحية المطلوبة (على سبيل المثال، البيانات والمعلومات المعرفة أو الغير المعرفة).

ثانيا. حساسية البيانات والمعلومات الصحية: بعض البيانات والمعلومات لها حساسية عالية ويجب توخي الحذر الشديد أثناء المشاركة. وهذا يشمل على سبيل المثال لا الحصر معلومات عن الإدمان على المواد الكيميائية ، وعدوى فيروس نقص المناعة البشرية ، وحالات الصحة العقلية ، وتقارير الصحة السلوكية (يمكن العثور على التفاصيل في: سياسة تصنيف أصول المعلومات الصحية).

ثالثا. الجدول الزمني للمعلومات (الأشهر والسنوات وما إلى ذلك)

رابعا. الغرض من مشاركة البيانات والمعلومات الصحية، وطريقة المشاركة ومدتها، وضوابط التخلص منها أو إتلافها.

خامسا. من سيصل إلى البيانات والمعلومات الصحية.

سادسا. ما هي البيانات الأخرى التي يتم جمعها مع المعلومات الصحية.

4.5. المتطلبات الأساسية لمشاركة المعلومات الصحية المحمية

4.5.1. يجب أن تخضع جميع مشاركة المعلومات الصحية المحمية لاتفاقية خاصة بمشاركة البيانات ويجب أن تفي بمتطلبات تشريعات السارية في الدولة والإمارة.

4.5.2. يجب تسجيل اتفاقيات مشاركة البيانات من قبل الجهة المختصة داخل المنشأة؛ ويجب تسجيل جميع تدفقات البيانات في سجل أصول المعلومات.

4.5.3. يجب مشاركة المعلومات الصحية المحمية فقط، وفق أحكام التشريعات السارية ومن قبل المصرح لهم بذلك بحسب طبيعة كل حالة، كما يجب أن يكون الوصول إلى المعلومات

الصحية المحمية هو وصول قائم على الدور مع آلية ذات مصداقية مناسبة. يجب على المنشأة مراقبة عمليات الوصول إلى المعلومات الصحية المحمية وتدقيقها بشكل منتظم.

4.5.4. يجب أن تصل المنشآت التي تريد مشاركة المعلومات الصحية المحمية إلى اتفاق بشأن معايير البيانات الأساسية ووصفها.

4.5.5. يجب فقط مشاركة الحد الأدنى من المعلومات الصحية المحمية الضرورية، ويجب التحقق من دقتها قبل الإصدار؛ لتجنب الأخطاء.

4.5.6. يجب فقط مشاركة البيانات والمعلومات الصحية عبر وسائل آمنة ومصرح بها، ويجب وضع الضمانات التقنية المناسبة لحماية المعلومات الصحية المحمية.

4.6. مشاركة المعلومات الصحية المحمية لأغراض الرعاية الصحية (الاستخدام الأولي)

4.6.1. يمكن لمتخصصي الرعاية الصحية مشاركة البيانات والمعلومات لصالح صاحب البيانات/ المرضى ضمن الإطار المنصوص عليه في القانون الاتحادي رقم (2) لسنة 2019 في شأن استخدام تقنية المعلومات والاتصالات في المجالات الصحية والقرارات الصادرة بموجبه، والسياسات المعتمدة لدى الهيئة بهذا الشأن سياسة حماية البيانات الصحية وسرية المعلومات.

4.6.2. يجب أن يكون الغرض الأساسي لمشاركة البيانات والمعلومات لصالح المريض الذي يتلقى رعاية صحية مباشرة، وقد يكون للفشل في مشاركة البيانات والمعلومات (بكفاءة وأمان) عواقب وخيمة على صحة صاحب البيانات/ المريض.

4.6.3. يجب أن تقتصر مشاركة المعلومات الصحية المحمية على الأشخاص المصرح لهم ووفق القنوات المحددة داخل المنشأة.

4.6.4. عندما يتم نقل رعاية/علاج المريض إلى منشاة أخري، يجوز نقل نسخة من الملف الطبي

مباشرة مع المريض/صاحب البيانات نفسه أو عن طريق طلب من المنشأة الأخرى (يلزم الحصول على موافقة المريض بشكل منفصل في هذه الحالة).

4.6.5. يوضح الجدول أدناه الحالات المختلفة التي يمكن مشاركة المعلومات الصحية المحمية فيها لأغراض الرعاية الصحية للمريض/صاحب البيانات:

الاستخدام الأساسي للمعلومات الصحية لغرض الرعاية الصحية		
بين المنشآت الصحية في إمارة دبي	نقل الملف الطبي بموافقة المريض	دخول منصة نابض بموافقة المريض
بين المنشآت الصحية في نفس المؤسسة بالدولة	يتوجب أخذ موافقة المريض	
بين المنشآت الصحية (ليست ضمن نفس المؤسسة) في الدولة	يقوم المريض بنقل معلوماته الصحية	• عملية الإحالة بموافقة موقعة واضحة • تبادل المعلومات عبر المنصات المعتبرة للتبادل (منصة نابض، رعايتي، ملفي) بموافقة المريض
المرضى الذين يتم علاجهم خارج الدولة في حدود الإجراءات العلاجية اللازمة	يتوجب أخذ موافقة المريض	
البيانات الصحية المتعلقة بالعينات التي يتم إرسالها إلى المختبرات خارج الدولة	يتوجب أخذ موافقة المريض	

4.7. مشاركة المعلومات الصحية المحمية لأغراض غير متعلقة بالرعاية الصحية (الاستخدام الثانوي للمعلومات الصحية)

4.7.1. يتعين على جميع المنشآت التي تشارك المعلومات الصحية المحمية بموجب التشريعات السارية والسياسات المعتمدة لدى الهيئة (سياسة حماية البيانات الصحية والسرية) ضمان

اتخاذ ما يلزم من إجراءات لحمايتها.

4.7.2. بالنسبة للبيانات المرتبطة بـ "مشروع الجينوم الوطني لدولة الإمارات العربية المتحدة"، يجب أن تكون وفقًا لإطار الوصول إلى بيانات مستودع الجينوم الوطني للدولة والسياسات ذات الصلة.

4.7.3. تقنيات التسمية المستعارة وإخفاء الهوية الفعالة تمكّن المنشأة من إجراء استخدام ثانوي للمعلومات الصحية المحمية بطريقة آمنة وقانونية. من خلال إزالة الهوية، يمكن للمستخدمين استخدام البيانات الفردية لمجموعة من الأغراض الثانوية دون الحاجة إلى الوصول إلى المعلومات الصحية المحمية القابلة للتحديد والتعرف على صاحب البيانات.

4.7.4. وفقًا للمادة (16) من القانون الاتحادي رقم (2) لسنة 2019 في شأن استخدام تقنية المعلومات والاتصالات في المجالات الصحية والمادة (4) من قانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية يجب على كل من يتداول البيانات والمعلومات الخاصة بالمرضى المحافظة على سريتها وعدم استخدامها لغير الأغراض الصحية دون موافقة خطية من صاحب البيانات/ المريض، باستثناء حالات معينة ووفقاً للتشريعات السارية.

4.7.5. يوضح الجدول أدناه بالتفصيل الاستخدام الثانوي للمعلومات الصحية المحمية:

مشاركة المعلومات الصحية المحمية لأغراض غير متعلقة بالرعاية/ الاستخدام الثانوي للمعلومات الصحية دون موافقة صاحب البيانات/ المريض	
غرض الاستخدام	**نوع المعلومات**
بناء على طلب الجهات القضائية المختصة.	المعلومات الصحية المعرفة
للتحقيق أو إنشاء أو ممارسة أو الدفاع عن الدعاوى القانونية أو الدعاوى القانونية المحتملة بما في ذلك الشكاوى المقدمة إلى التنظيم الصحي ضد المنشأة أو موظفيها ؛ أو عند طلب المحاكم بصفتها القضائية.	
المعلومات الصحية التي تطلبها شركات التأمين الصحي أو شركات إدارة المطالبات أو أية جهة ممولة للخدمات الصحية فيما يتعلق بالخدمات الصحية التي يتلقاها المريض، لأغراض المراجعة أو الموافقة أو التحقق من الاستحقاقات المالية المتعلقة بتلك	

الخدمات.	
بناءً على طلب السلطات الصحية (وزارة الصحة ووقاية المجتمع وهيئة الصحة في دبي) 1. لاتخاذ الإجراءات الوقائية والعلاجية المتعلقة بالصحة العامة 2. الحفاظ على صحة وسلامة المريض أو أي شخص آخر على اتصال به (على سبيل المثال الحماية من الأمراض المعدية/ الأوبئة والتهديدات الخطيرة للصحة). 3. في حالات الطوارئ المتعلقة بالسلامة العامة للحفاظ على صحة وسلامة أصحاب البيانات/المرضى أو أسرهم أو أي أشخاص آخرين على اتصال بهم، أو المجتمع بشكل أوسع.	
بناءً على طلب السلطات الصحة العامة (وزارة الصحة ووقاية المجتمع وهيئة الصحة بدبي) المخولين قانونًا لتلقي التقارير بغرض منع أو السيطرة على المرض أو الإصابة أو الإعاقة.	
بناءً على طلب الهيئة لأغراض الرقابة والتفتيش وإدارة المخاطر والتدقيق و إدارة الأخطاء.	
لتحديد مدى توافر خدمات الرعاية الصحية وجودتها وسلامتها وإنصافها وفعاليتها من حيث التكلفة.	المعلومات الصحية الغير معرفة
بناءً على طلب الهيئة لتحليل أو تجميع المعلومات الإحصائية فيما يتعلق بإدارة أو تقييم أو مراقبة أو تخصيص الموارد أو التخطيط لكل أو جزء من النظام الصحي بما في ذلك تقديم الخدمات.	
لأغراض البحث العلمي والسريري بشرط عدم الكشف عن هوية المرضى و اتباع أخلاقيات وقواعد البحث العلمي وفقًا لمبادئ وإرشادات ICH_GCP.	المعلومات الصحية الغير معرفة إذا كانت هناك حاجة إلى المعلومات الصحية المعرفة، فيجب الحصول على موافقة المريض مسبقاً
لأنشطة التطوير والابتكار أو السجلات الصحية	

4.8. مشاركة المعلومات الصحية المحمية

4.8.1. يجب أن تخضع مشاركة أي معلومات صحية محمية بقواعد واضحة تفي بمتطلبات التشريعات في الدولة ولوائح الهيئة لتمكين الممارسات الفعالة من قبل كل من الأطراف المفصح عنها والمتلقي.

4.8.2. يجب أن تدعم المنشأة حقوق الأفراد فيما يتعلق بمشاركة معلوماتهم الصحية المحمية. يجب أن تحدد المنشأة التزامات عالية المستوى لحماية المعلومات الصحية المحمية؛ خاصة فيما يتعلق بكيفية مشاركة المعلومات الصحية المحمية (داخليًا وخارجيًا).

4.8.3. حددت الهيئة سلسلة من الحقوق والتعهدات لصاحب البيانات/ المريض عبر سياسة حماية البيانات والمعلومات الصحية وخصوصيتها والتي يتعين على جميع المنشآت الخاضعة لسلطاتها الامتثال لها. وهذا يشمل احترام حق الفرد في الحفاظ على خصوصيته وسريته، وتوقع أن تحتفظ المنشأة بمعلوماته السرية (الخاصة به) بطريقة آمنة.

4.8.4. يجب على المنشأة التأكد من أن جميع عمليات نقل/ مشاركة المعلومات داخل المنظومة أو خارجها محمية ببروتوكولات مشاركة المعلومات المناسبة وأن استلام ونقل جميع المعلومات السرية والمعلومات السرية الخاصة بالمنشأة يحدث ضمن حدود تشريعات الدولة ولوائح الهيئة.

4.8.5. يجب الحصول على الموافقة حسب الاقتضاء من صاحب البيانات/ المريض قبل مشاركة المعلومات الصحية المحمية وفقًا لهذه السياسة.

4.8.6. يجب أن تكون هناك مراجعات/ تدقيق منتظم لممارسات مشاركة المعلومات الصحية المحمية في المنشأة.

4.9. مشاركة المعلومات الصحية المحمية مع الشرطة

4.9.1. يمكن الكشف عن المعلومات الصحية المحمية للشرطة من أجل المساعدة في منع الجريمة أو اكتشافها و/ أو القبض على مرتكبي الجرائم.

4.9.2. إذا كان الشخص موضوع الطلب متاحًا وقادرًا، فيجب أن يُطلب منه تقديم موافقته على الكشف عن المعلومات المطلوبة.

4.9.3. إذا كان الشخص موضوع الطلب ليس قادرًا على تقديم الموافقة (على سبيل المثال وليس الحصر صاحب البيانات/ المريض مغمي عليه؛ أو يعاني من إعاقة ذهنية؛ أو لديه عجز عقلي) ؛ أو إذا كان صاحب البيانات/ المريض قاصراً (أقل من 18 عاماً)، يلزم توقيع ولي الأمر أو الوصي القانوني على الموافقة لمشاركة البيانات الصحية المحمية.

4.9.4. لكي ينظر المنشأة في مشاركة أي معلومات صحية دون موافقة صاحب البيانات/المريض، يجب أن يتعلق الطلب بجريمة خطيرة، وإلا فيجب أن يُطلب من الشرطة الحصول على أمر من المحكمة أو موافقة كتابية موقعة من صاحب البيانات/ المريض.

4.9.5. يجب تقديم جميع الطلبات المقدمة من الشرطة كتابيًا (نسخة إلكترونية أو ورقية)، ومن الأفضل تقديمها بشكل رسمي مع تقديم الوثائق المطلوبة.

4.9.6. يجب أن يتم التعامل مع الطلبات من قبل فريق حوكمة البيانات في المنشأة لمراجعة/ رفض/ أو قبول الطلب.

4.9.7. في بعض الأحيان قد يتم تقديم طلبات عاجلة تتطلب تقديم معلومات محددة في فترة زمنية قصيرة. ويرجع ذلك في كثير من الأحيان إلى الجداول الزمنية الصارمة المفروضة على الشرطة لاتخاذ قرارات لتوجيه الاتهام إلى المشتبه بهم أو دعم إجراءات التحقيق العاجلة. في هذه الظروف، ينبغي اتخاذ القرارات من قبل المدير الطبي للمنشأة و/ أو الفريق القانوني للمنشأة

قبل أي إفصاح عن المعلومات.

4.9.8. يجب حفظ نسخة من الطلب المقدم من الشرطة والقرار المتخذ بشأنه وأي معلومات مقدمة للشرطة في الملف الطبي لصاحب البيانات/ المريض.

4.10. مشاركة المعلومات الصحية المحمية من خلال رسائل البريد الإلكتروني

4.10.1. يسمح إرسال المعلومات الصحية المحمية عبر البريد الإلكتروني بعد أن يتم تشفيرها بشكل مناسب أو إذا كان البريد الإلكتروني يحتوي على روابط لبيانات المريض داخل البوابة الرقمية للمرضى التي يتم حماية الدخول إليها من خلال آلية التحقق من هوية المستخدم.

4.10.2. يجب استخدام حسابات البريد الإلكتروني الرسمية الصادرة عن المنشأة فقط لإرسال المعلومات الصحية المحمية أو مناقشتها.

4.10.3. لا ينبغي أبدًا استخدام عناوين البريد الإلكتروني الشخصية/الخاصة من قبل الموظفين لأي غرض/عمل تابع للمنشاة في مشاركة البيانات الصحية المحمية.

4.10.4. عند إرسال البريد الإلكتروني من حساب المنشأة إلى مجال مدرج في القائمة الآمنة لتكنولوجيا المعلومات، يجب تشفير البريد الإلكتروني وأي مرفقات خاصة بالبريد تلقائيًا؛ يجب تطبيق نفس النمط أيضًا بالنسبة لرسائل البريد الإلكتروني المرسلة بين المنشآت. حيث يجب تشفير رسائل البريد الإلكتروني المرسلة إلى أي عنوان آخر يدويًا وإضافة كلمة "(تشفير)" في عنوان موضوع البريد الإلكتروني.

4.11. مشاركة المعلومات الصحية المحمية من خلال الوسائط المتعددة القابلة للإزالة (وحدات USB ، الأقراص المضغوطة/ أقراص DVD وغيرها)

4.11.1. يتوجب عدم تخزين المعلومات الصحية المحمية على وسائط قابلة للإزالة ما لم يكن ذلك

ضروريًا للغاية مع إلزام خاصية التشفير. إذا كان هناك شرط لاستخدام الوسائط القابلة للإزالة، فيجب على مقدم الرعاية الصحية مناقشة الخيارات المتاحة مع الجهة المختصة في المنشأة.

4.11.2. عندما يكون استخدام الوسائط القابلة للإزالة مطلوبًا وموافقًا عليه، يجب الاحتفاظ بالمعلومات على الجهاز فقط لأدنى فترة ممكنة (يجب نسخ المعلومات احتياطيًا إلى وحدة تخزين متصلة بالشبكة إذا كانت ستبقى على الجهاز لأكثر من عملية نقل بسيطة بين أنظمة المنشآت).

4.11.3. يجب استخدام جهاز مشفر معتمد من المنشأة فقط ويجب حماية الأمان المادي للجهاز.

4.11.4. يجب أن يتم تبادل الأجهزة من خلال موظفين محددين فقط.

4.11.5. يجب التوقيع على اتفاقية عدم الإفصاح (NDA) بشكل متبادل في حالة نقل الوسائط المتعددة القابلة للإزالة، عند إدارتها من خلال أطراف خارجية.

4.12. تبادل المعلومات الصحية المحمية عبر الفاكس

4.12.1. لا يتم تشجيع إرسال الفاكس كطريقة لنقل المعلومات الصحية المحمية لأسباب تتعلق بخصوصية المعلومات وسريتها.

4.12.2. يجب إرسال المعلومات الشخصية والسرية عن طريق الفاكس فقط عندما يكون ذلك ضروريًا للغاية، ولا توجد طريقة بديلة للنقل.

4.12.3. يجب دائمًا مراعاة استخدام البريد الإلكتروني الآمن أولاً، قبل إرسال المعلومات عن طريق الفاكس. عندما يكون من الضروري للغاية إرسال رسالة فاكس، يجب إرسالها باستخدام الإجراءات الآمنة كما هو موضح أدناه:

أ. يجب إرسال الفاكس إلى مكان آمن حيث يتمكن من الوصول إليه الأفراد الذين لديهم صلاحية الوصول إلى المعلومات فقط.

ب. يجب عدم ترك رسائل الفاكس السرية الواردة والصادرة في مكان حيث يمكن للأشخاص غير المصرح لهم رؤيتها.

ج. يجب أن تتضمن أي رسائل فاكس يتم إرسالها ورقة غلاف تحمل علامة "خاصة وسرية" وتحتوي على بند السرية الملائم.

د. يجب أن يكون المرسل على يقين من أن الشخص الصحيح سيتلقى الفاكس. يجب إخطار المستلم عند إرسال الفاكس ويجب أن يُطلب منه الإقرار بالاستلام. إذا أمكن، يجب تحضير تقرير لتأكيد الإرسال الموفق.

ه. يجب على الموظفين التأكد من صحة رقم الفاكس وتوخي الحذر عند الاتصال. حيثما أمكن، يجب استخدام الأرقام المبرمجة مسبقًا (والتحقق بانتظام من أي تغييرات).

و. يجب إدراج الحد الأدنى فقط من المعلومات الشخصية والمعرفة في رسالة الفاكس. حيثما أمكن، يجب أن تكون المعلومات مشفرة أو مخفية الهوية. إذا تم استلام مستند بشكل غير صحيح داخل المنشأة، فإنه يقع على عاتق القسم/ الإدارة المتلقي مسؤولية التأكد من أنه قد تم تسليمه إلى المستلم المحدد وإخطار المرسل بالخطأ. يجب أيضًا تسجيل الخطأ كتابيا في القسم المعني.

4.13. تبادل المعلومات الصحية المحمية من خلال البريد/ البريد السريع

4.13.1. يجب أن تكون الأظرف التي تحتوي على معلومات صحية محمية مغلقة بإحكام وموجهة إلى شخص معين ويجب توخي الحذر من قبل الموظفين للتأكد من أن الأظرف لا تحتوي على معلومات غير مخصصة للمستلم.

4.13.2. يجب توخي الحذر لضمان توثيق البريد الداخلي والخارجي بشكل صحيح على الطرد البريدي وتغليفها بشكل مناسب.

4.13.3. عند إرسال معلومات حساسة أو سرية للغاية، ينبغي توخي الحذر في طريقة النقل ومدى ملاءمة مواد التعبئة والتغليف. عند الإرسال عن طريق البريد الخارجي، يجب أن يكون ذلك عبر طرق آمنة حيث يمكن تتبع الطرد البريدي وتوقيعها عند الاستلام من قبل الشخص المستلم.

4.13.4. يجب تجنب إرسال معلومات سرية للغاية عن طريق البريد - يجب تسليمها باليد حيثما أمكن ذلك. عند نقل المعلومات الصحية المحمية باليد، يجب تغليفها بشكل مناسب لتجنب ضياع المعلومات أو رؤيتها بشكل غير لائق.

4.13.5. يمكن فقط استخدام الشركات التي لديها عقد تجاري قائم مع المنشأة (مع بنود حوكمة المعلومات المناسبة فيما يتعلق بحماية البيانات، بما في ذلك اتفاقية عدم الإفصاحNDA ، ضمن العقد) لنقل معلومات المرضى أو الموظفين أو المعدات أو الأدوية أو الوثائق. يجب أن يتم تسجيل الدخول والخروج على أي معلومات محمية صحية يتم نقلها بهذه الطريقة بشكل مناسب ونسخ دليل الإرسال/ الاستلام المحتفظ به.

4.13.6. في الأماكن العامة، يجب فتح البريد الوارد بعيدًا عن روية عامة الناس وعدم تركه بدون إشراف.

4.13.7. عند الاقتضاء، يجب التحقق من الهوية قبل تسليم الطرد البريدي الذي يحتوي على معلومات صحية محمية إلى صاحب البيانات (المريض) أو الشخص المرخص له.

4.14. تبادل المعلومات الصحية المحمية من خلال الهواتف/ أجهزة الرد الآلي/ رسائل الهاتف/ المحادثات الشفوية

4.14.1. عند مشاركة المعلومات الصحية المحمية عبر الهاتف، يجب على الموظفين عدم تشغيل رسائل الرد على الهاتف على مكبر الصوت في الأماكن العامة أو الأماكن التي يوجد فيها

شكوك من أن يسمعها أفراد غير مصرح لهم.

4.14.2. قبل التصريح عن أي معلومات إلى المتصل الذي يدعي أنه صاحب البيانات أو المريض المعني، يجب على الموظفين التأكد بشأن هوية المتصل من خلال الحصول على بعض التفاصيل الشخصية (مثل تاريخ الميلاد أو العنوان أو الرمز البريدي أو تواريخ الموعد أو تفاصيل العلاج/ العيادة أو رقم الملف الطبي). قد يختار صاحب البيانات/ المريض تطبيق حماية إضافية لسجله الطبي الإلكتروني عن طريق توفير كلمة مرور (قام صاحب البيانات بإعطائها مسبقاً) من قبل أي متصل قبل إعطاء أي معلومات صحية محمية.

4.14.3. إذا كان لا يمكن التحقق من هوية صاحب البيانات/ المريض فلا ينبغي الإفصاح عن أي معلومات.

4.14.4. يجب أن يكون الموظفون على دراية بشأن صاحب البيانات/ المريض الذي تم وضع علامة على سجلاته الطبية الإلكترونية مع تنبيه يوضح الحاجة إلى حماية إخفاء الهوية أو إجراءات حماية إضافية. يجب وضع أي متصل يطلب معلومات حول صاحب البيانات/ المريض الذي تم الإبلاغ عنه في انتظار وطلب المشورة الفورية من الإدارة العليا في المنشأة.

4.14.5. يجب الكشف عن المعلومات الصحية المحمية المتعلقة بالمرضى في العيادات الخارجية للمنشأة فقط للأفراد المصرح لهم بتلقي المعلومات من قبل صاحب البيانات/ المريض (مثل أقرب الأقارب أو الوصي القانوني).

4.14.6. بالنسبة للمرضى الداخليين في المنشأة، يجب توجيه جميع المكالمات إلى الجناح/ القسم حيث يوجد صاحب البيانات/ المريض ما لم يكن هناك تنبيه يمنع ذلك. لذلك، من الضروري رفع وتسجيل أي حالة خاصة تتعلق بحالات المريض الداخلي بشكل مناسب.

4.14.7. يتوجب عدم الكشف عن البيانات أو المعلومات إلى أي شخص إلا بعد الحصول على موافقة صاحب البيانات/ المريض أو عندما لا يكون ذلك قابلاً للتطبيق بسبب حالة المريض (على

سبيل المثال، حالات الطوارئ التي تهدد الحياة مع عدم كفاية الوقت للحصول على الموافقة). من المهم ملاحظة أن أقرب الأقارب ليس لديهم أي حق تلقائي للوصول إلى معلومات المريض الصحية المحمية. بيد أن للوالدين/ أولئك الذين لديهم مسؤولية أبوية الحق في الحصول على معلومات عن صحة أطفالهم.

4.14.8. كجزء من عملية إدخال المرضى، قد يُسأل المرضى مسبقًا عما إذا كانوا يرغبون في مشاركة المعلومات الصحية حول رعايتهم مع شخص مفوض معين من قبلهم. يمكن بعد ذلك مشاركة المعلومات مع هذا الشخص، إما شخصيًا أو عبر الهاتف، دون الحاجة إلى الحصول على موافقة أخرى. عندما يتم تأكيد مفوض معين، يجب تسجيل تفاصيل الاتصال الخاصة به في الملف الطبي الإلكتروني للمريض لضمان اتباع رغبات المريض باستمرار.

4.15. العمل عن بعد (المنزل، خارج موقع المنشأة، إلخ.)

4.15.1. الموظفون مسؤولون عن سرية وأمن أي بيانات أو معلومات يحتفظون بها عن بعد بشكل ورقي أو إلكتروني، وعن نقلها من وإلى مقر المنشأة.

4.15.2. يجب أن يتأكد الموظفون من أنهم يحتفظون بالحد الأدنى فقط من المعلومات الصحية المحمية عند العمل عن بُعد، وأن يتأكدوا من الامتثال لسياسات تكنولوجيا المعلومات وأمن المعلومات وحوكمة البيانات ذات الصلة.

4.15.3. يجب أن تكون الأجهزة المستخدمة في بيئة العمل عن بعد محمية للغاية فيما يتعلق بالجوانب الأمنية ويجب التأكد من عدم تخزين المعلومات الصحية المحمية للمرضى على تلك الأجهزة؛ لتقليل مخاطر خرق البيانات في حالة فقد الجهاز أو سرقته.

4.15.4. لا يجوز للموظفين استخدام أجهزتهم الشخصية للعمل عن بُعد ويجب استخدام الأجهزة المقدمة من المنشأة دائمًا للاتصال عن بُعد للأغراض المتعلقة بالعمل.

4.16. الوصول إلى المعلومات الصحية المحمية من قبل الطبيب المقيم في تخصصات الطب البشري وطب الأسنان وطلاب الرعاية الصحية والباحثين والمدققين السريريين

4.16.1. الطبيب المقيم في تخصصات الطب البشري وطب الأسنان

يسمح للطبيب المقيم في تخصصات الطب البشري وطب الأسنان المسجلين في نظام شريان التابع للهيئة والعاملين ضمن فريق الرعاية الصحية الذي يقدم (أو يدعم) رعاية المريض، الوصول إلى المعلومات الصحية المحمية للمريض حالهم كحال أعضاء الفريق الآخرين، ما لم يعترض صاحب البيانات/ المريض.

4.16.2. طلاب ومتدربي الطب البشري/ طب الأسنان/ التمريض/ الطب المساعد

يمكن للطلاب والمتدربين في مجالات الرعاية الصحية تحت إشراف مقدمي الرعاية الصحية المسجلين في نظام شريان رؤية المعلومات الصحية المحمية للمريض كقراءة فقط مع الإشراف المناسب.

4.16.3. الباحثين والمدققين السريريين

أ. يجب على المنشأة التأكد من وجود أنظمة التصريح للمشاريع البحثية وأن لجان الأخلاقيات البحث العلمي ولجان التدقيق على دراية بمسؤوليات الطاقم الطبي والباحثين فيما يتعلق بالسرية وتعزيز الممارسات الجيدة.

ب. من المستحسن أن تكون البيانات المتوفرة للأبحاث أو التدقيق غير معرفة ما لم يكن ذلك ضروريًا؛ ويجب أن يمر هذا بإجراءات خاصة للموافقة والتدقيق.

ج. يجب إخفاء هوية البيانات التي يتم مشاركتها مع الباحثين المتعاونين الخارجيين أو الإحصائيين للتجارب السريرية والبحوث؛ يجب إزالة جميع المعرفات المباشرة من مجموعة البيانات والمعرفات شبه المعدلة.

4.17. استخدام المعلومات الصحية المحمية لغرض التدريس

4.17.1. لا ينبغي استخدام المعلومات الصحية المحمية كمجموعة بيانات لأغراض التدريس دون موافقة صاحب البيانات/ المريض.

4.17.2. المعلومات الغير حقيقية هي أنسب مجموعة بيانات يمكن استخدامها لهذا الغرض، حيث لا يمكن التعرف على شخص حقيقي من المعلومات المستخدمة. بدلاً من ذلك، يمكن استخدام المعلومات مجهولة المصدر حول صاحب البيانات/ المرضى والحالات الطبية للتثقيف والتدريب الصحي. يجب أن يكون هناك تحكم مناسب للتأكد من إجراء إخفاء الهوية بشكل صحيح.

4.17.3. إذا تم استخدام المعلومات أو الوسائط التي يمكنها (بشكل مباشر أو غير مباشر) تحديد هوية الفرد، فيجب الحصول على الموافقة من صاحب البيانات/ المريض.

4.17.4. عند وجود احتمالية استخدام المعلومات الصحية المحمية لأغراض التدريس/ التدريب في المستقبل، يجب إبلاغ صاحب البيانات/ المريض خلال جمع البيانات والحصول على الموافقة المناسبة منه/ منها.

4.18. استخدام المعلومات الصحية المحمية لاختبار النظام

4.18.1. يجب على المنشآت تجنب استخدام المعلومات الصحية المحمية لاختبار النظام.

4.18.2. في حالة عدم وجود طريقة عملية بديلة لاستخدام البيانات المحمية لهذا الغرض يجب على الأشخاص المعنيين في إدارة النظام تطوير تدابير أمنية مناسبة لحماية المعلومات الصحية المحمية من الوصول غير المصرح به، والكشف عن هوية صاحب المعلومات الصحية المحمية، أو فقدان البيانات. يفضل أن تكون المعلومات الصحية مخفية الهوية؛ من خلال إزالة البيانات التعريفية الخاصة (على سبيل المثال: الاسم والعنوان ورقم الملف الطبي ورقم الهاتف وما إلى

ذلك) واستبدالها ببيانات عامة. الطريقة الأكثر أمانًا للتعامل مع هذه الحالة هي استخدام أدوات إنشاء بيانات الاختبار المؤتمتة المصممة لدعم الأداء الجيد لمجموعات البيانات الكبيرة.

4.18.3. قبل البدء في أي اختبار للنظام باستخدام البيانات المحمية، يجب على الموظفين إجراء تقييم تأثير حماية البيانات (DPIA).

4.19. مشاركة المعلومات الصحية المحمية مع أطراف ثالثة في القطاع الخاص داخل الدولة للمعالجة

4.19.1. إذا أمرت المنشأة طرفًا ثالثًا، داخل الدولة، بمعالجة المعلومات الصحية المحمية نيابة عنها، فيجب توقيع اتفاقيات/ عقد مشاركة البيانات.

4.19.2. يجب أن تتضمن اتفاقية/ عقد مشاركة البيانات فقرات واضحة تحدد مسؤوليات حماية البيانات والمعلومات الصحية وسريتها، بما يتوافق مع قوانين الدولة ومتطلبات سياسات الهيئة. في حالة عدم وجود مثل هذا الشرط في اتفاقية/ عقد مشاركة البيانات، يجب على معالج البيانات إكمال اتفاقية سرية منفصلة والتوقيع عليها.

4.19.3. يجب على المنشأة التأكد من أن المعالج يقدم "ضمانات كافية" لوجود تدابير أمنية تقنية ومؤسسية مناسبة لحماية سرية المعلومات الصحية المحمية.

4.19.4. يجب على معالج البيانات والمعلومات الصحية الالتزام بشروط حماية البيانات والمعلومات الصحية وسريتها حتى بعد انقضاء مدة العقد.

4.19.5. يجب على المنشأة (كمراقب البيانات والمعلومات الصحية) ضمان حماية المعلومات الصحية المحمية المستلمة من أطراف ثالثة أو تبادلها معها وفقًا للمتطلبات التشريعية والتنظيمية للدولة والهيئة، بما في ذلك هذه السياسة.

4.19.6. أي بيانات أو معلومات صحية منقولة من قبل المنشأة إلى خارج المؤسسة (ولكن داخل الدولة)

للمعالجة، يجب تشفيرها بشكل آمن أثناء النقل.

4.19.7. في حال ضرورة نقل المعلومات الصحية المحمية من خلال أي وسائط إلكترونية محمولة، يجب تنفيذ هذه العملية مع الحفاظ على أمان وسرية المعلومات بشكل صارم، ويجب تشفير جميع الوسائط الإلكترونية المحمولة.

4.19.8. عندما يتم نقل المعلومات الصحية المحمية إلكترونيًا، يجب أن تلتزم المنشأة بإجراءات التحكم في الوصول المتعلقة بالخصوصية والأمان والسرية (مثل البوابات المحمية بكلمة مرور وطبقة مآخذ التوصيل الآمنة المشفرة (SSL))

4.19.9. عند معالجة المعلومات الصحية المحمية بواسطة طرف ثالث، يجب عدم الاحتفاظ بالمعلومات لفترة أطول من اللازم.

4.20. نقل المعلومات الصحية المحمية إلى خارج دولة الإمارات العربية المتحدة

4.20.1. يجب عدم تخزين أو نقل المعلومات الصحية المحمية إلى خارج الدولة ؛ باستثناء الحالات الواردة في قرار مجلس الوزراء رقم (51) لسنة 2021 بشأن الإعفاء لتخزين ونقل السجلات والمعلومات الصحية بشأن الحالات التي يجوز فيها تخزين أو نقل البيانات والمعلومات الحية خارج الدولة.

4.20.2. يجب الحصول على موافقة الهيئة وفقًا ل سياسة تصنيف أصول المعلومات الصحية

4.20.3. يمكن منح الموافقة عن طريق إرسال الطلب إلى: HISH@dha.gov.ae

4.20.4. يجب أن يتم نقل أو مشاركة المعلومات الصحية المحمية إلى خارج الدولة بشكل آمن لمنع مخاطر الكشف العرضي عن هوية صاحب البيانات أو إتلاف المعلومات أثناء النقل.

4.20.5. يجب تشفير المعلومات الصحية المحمية بشكل آمن أثناء النقل؛ ويجب الالتزام بالإجراءات الأمنية اللازمة.

4.21. اتفاقيات مشاركة البيانات والمعلومات الصحية

4.21.1. يجب أن تخضع جميع مشاركة البيانات والمعلومات الصحية مع المؤسسات خارج المنشأة لإتفاقية مشاركة البيانات والمعلومات الملاءمة التي تشتمل على ضوابط الخصوصية والأمان؛ وبنود قوية حول حوكمة البيانات والمعلومات حسب الإجراءات المعمول بها في الهيئة.

4.21.2. يجب أن تمتثل اتفاقية مشاركة البيانات والمعلومات الصحية لتشريعات الدولة ذات الصلة وسياسات الهيئة؛ ويجب أن تؤكد من يتحمل المسؤولية والتحكم في البيانات والمعلومات.

4.21.3. يجب أن تحدد اتفاقية مشاركة البيانات والمعلومات الصحية الشروط والأحكام بما في ذلك التفاصيل حول:

أ. جميع الأغراض المقصودة/ المحددة التي يتم من أجلها مشاركة البيانات والمعلومات الصحية.

ب. أنواع ووصف البيانات والمعلومات التي سيتم مشاركتها، (قد يلزم إرفاق هذا كقائمة من حقول البيانات)، وكيفية إخفاء الهوية/ طمس الهوية، وعدد عمليات النقل للمعلومات. يجب أن تكون البيانات والمعلومات التي يتم مشاركتها كافية وذات صلة ومقتصرة لما هو ضروري فيما يتعلق بالأغراض التي من أجلها تم مشاركتها، لمنع الإفصاح عن معلومات إضافية أو غير ذات صلة.

ج. تحديد أدوار كل طرف؛ نوع السلطة التي سيحصلون عليها على مشاركة البيانات والمعلومات الصحية، والمستلمين المحتملين/ أو أنواع المستلمين والحالات التي سيتمكنون فيها من الوصول إلى البيانات والمعلومات المشاركة.

د. وصف حول مدة الاحتفاظ بالبيانات والمعلومات الصحية المشاركة، وإجراءات التعامل مع الحالات التي قد يكون فيها للمنشآت /المؤسسات المختلفة مدة احتفاظ متفاوتة.

ه. شرح ترتيبات التخلص/ التدمير؛ بما في ذلك حذف البيانات والمعلومات المشاركة أو إعادتها

إلى المنشأة/ المؤسسة التي زودت البيانات في الأصل.

ز .تفاصيل حول متطلبات ضوابط الخصوصية والأمان للمنشأة/ المؤسسة التي تتلقى البيانات والمعلومات الصحية، كيف سيتم تخزين البيانات والمعلومات الصحية ونقلها؛ وإجراءات التعامل مع أي خرق للاتفاقية.

ح. تفاصيل عن الجدول الزمني لتقييم الفعالية المستمرة لاتفاقية مشاركة البيانات والمعلومات الصحية وإجراءات التعامل مع إنهاءها، بما في ذلك حذف البيانات والمعلومات الصحية المشاركة أو إعادتها إلى المنشأة الذي وفرت البيانات والمعلومات في الأصل.

ط. السمات الخاصة بخطة الاستجابة للحوادث لكلا المنشأتين (المتحكم والمعالج) التي تتناول مراحل مثل الإعداد والتعرف والاحتواء والقضاء على الحوادث، واسترداد البيانات والمعلومات والدروس المستفادة. يجب أن تتضمن اتفاقية مشاركة البيانات والمعلومات الصحية نبذة عن المتطلبات التي يجب على معالج المعلومات الصحية المحمية اتباعها ومسؤوليته عن أي حوادث مرتبطة بفقدان البيانات الشخصية أو الوصول غير المصرح به إليها. ستحتاج المعالجات الفرعية أيضًا إلى الامتثال لسياسات الهيئة بناءً على كل علاقة تعاقدية قائمة بين المعالج والمعالج الفرعي.

ي. تفاصيل عن المنشآت/ المؤسسات التي ستشارك في مشاركة البيانات والمعلومات جنبًا إلى جنب مع تفاصيل الاتصال الكاملة لأعضائها الرئيسيين (الأشخاص المسؤولين). إذا كان هناك عقد واحد أو أكثر مرتبطًا بالاتفاقية، فيجب الرجوع إليها أيضًا.

ك. القاعدة الشرعية لمشاركة البيانات والمعلومات. إذا كانت موافقة المريض مطلوبة، فكيف سيتم تسجيلها وإدارتها وكيف سيتم إبلاغ صاحب البيانات/ المريض بشأن مشاركة المعلومات الخاصة به/ بها.

ل. حقوق صاحب البيانات/ المرضى بما في ذلك إجراءات التعامل مع طلبات الوصول إلى

البيانات والمعلومات.

م. الترتيبات العامة بحوكمة البيانات والمعلومات الصحية - على سبيل المثال، إذا تم استبدال منشاة/ مؤسسة مشاركة بأخرى عند إعادة شراء الخدمات.

س. العقوبات والتبعات القانونية لعدم الامتثال للاتفاقية أو الانتهاكات من قبل الموظفين/ أي من الطرفين.

4.21.4. يجب على المنشأة مراجعة جميع اتفاقيات مشاركة البيانات والمعلومات الصحية بشكل منتظم، لكي تتطابق مع التحديثات في التشريعات والقوانين السارية في الدولة، ويجب أن تنعكس هذه التحديثات في الاتفاقية لضمان تبرير المشاركة.

4.21.5. قبل الدخول في أي اتفاقية لمشاركة البيانات والمعلومات الصحية، يجب إجراء تقييم لأثر حماية البيانات (DPIA) من أجل تقييم الفوائد التي قد تجلبها مشاركة المعلومات للأفراد أو المجتمع.

4.22. مخاطر إعادة تحديد هوية صاحب البيانات / المريض

4.22.1. لمنع مخاطر إعادة تحديد هوية أصحاب البيانات للمعلومات المشفرة أو المخفية، يجب على المنشأة (كونها المتحكمة على المعلومات الصحية المحمية) تطوير أفضل الممارسات والإجراءات لضمان أمن المعلومات وحماية خصوصية أصحاب البيانات.

4.22.2. يمكن أن تكون إمكانية ربط العديد من مجموعات البيانات والمعلومات ذات الأسماء المستعارة مع نفس الفرد ~~متحدة~~ لإعادة تحديد الهوية المريض/صاحب البيانات. يجب مناقشة أي مخاوف تتعلق بإعادة تحديد الهوية مع مكتب أمن المعلومات/ إدارة البيانات التابع للمنشأة قبل مشاركة أي بيانات أو معلومات.

4.23. يجب على جميع المنشآت الصحية

4.23.1. وضع سياسة وإجراءات مشاركة البيانات والمعلومات الصحية لضمان التعامل مع جميع المعلومات الصحية المحمية المشتركة ضمن مبادئ حماية البيانات الخاضعة لتشريعات وقوانين الدولة وسياسات ولوائح الهيئة بطريقة آمنة وخصوصية.

4.23.2. يجب مراجعة السياسات والإجراءات على فترات منتظمة (مرة واحدة على الأقل كل عامين) أو كلما كان هناك تغيير في تشريعات الدولة وسياسات ولوائح الهيئة؛ للحفاظ على امتثالها للتشريعات الحديثة.

4.23.3. تقع على عاتق مدير المنشأة مسؤولية التأكد من قيام مسؤول حوكمة المعلومات بإنفاذ السياسات والإجراءات المطلوبة داخل منشاته وأن جميع الموظفين على دراية بمسؤولياتهم المؤسسية والفردية فيما يتعلق بمشاركة المعلومات الصحية المحمية.

4.23.4. يجب أن يكون لدى جميع المنشآت تدابير مناسبة للتحقيق والتعامل مع المشاركة غير الملائمة أو غير المصرح بها للمعلومات الصحية المحمية سواء كانت متعمدة أو غير مقصودة:

أ. يجب التحقيق في هذه الحوادث على الفور لمعرفة السبب.

ب. يجب اتخاذ إجراءات تأديبية ضد الشخص (الأشخاص) المسؤول، إذا كان ذلك مناسبًا.

ج. يجب اتخاذ الخطوات المناسبة لتجنب التكرار.

د. يجب الإبلاغ عن خرق المعلومات الصحية إلى كل من مكتب البيانات للدولة والهيئة (datacompliance@dha.gov.ae) في غضون 24-48 ساعة. يمكن العثور على تفاصيل تنسيق/ محتوى الإخطار في سياسة حماية البيانات والمعلومات الصحية وخصوصيتها.

4.23.5. يجب على المنشآت تطبيق العقوبات المناسبة ضد الموظفين والمتدربين ومزودي الخدمة والمتعاقدين الخارجيين الذين ينتهكون سياسات وإجراءات مشاركة البيانات والمعلومات

الصحية.

4.23.6. المنشأة مسؤولة عن إثبات امتثالها لتشريعات وقوانين الدولة وسياسات ولوائح الهيئة؛ وسيُطلب منها تقديم أدلة تثبت استيفائها لنظام مشاركة البيانات والمعلومات الصحية المطلوب إلى الهيئة.

4.23.7. ضوابط المراجعة والتدقيق مطلوبة لتتبع جميع المعلومات الصحية المحمية التي تشاركها المنشأة مع الآخرين؛ ويجب الاحتفاظ بهذه السجلات لمدة 6 سنوات على الأقل بعد انتهاء اتفاقية المشاركة.

4.24. تطبيق السياسة

4.24.1. يتوجب على المنشآت تدريب جميع الموظفين والأفراد المتعاملين معها (المتدربين ومزودي الخدمة، الشركات المتعاقدة معها وأي شخص أخر مرتبط بمعاملة البيانات الصحية في المنشأة)، على سياسات وإجراءات مشاركة البيانات والمعلومات الصحية الخاصة بهم، ووفقاً لما تقتضيه الضرورة والملاءمة لأداء المهام.

4.24.2. لا ينبغي التعامل مع المعلومات الصحية المحمية أو استخدام الأنظمة حتى يتم الانتهاء من التدريب المناسب. يتعين على جميع أفراد القوى العاملة الخضوع للتدريب الأمني والتوعوي قبل الوصول إلى المعلومات الصحية المحمية.

4.24.3. يجب على المنشأة مراجعة الدورات التدريبية والتوعوية بشكل دوري لتعكس قوانين الدولة الحالية والمتطلبات التنظيمية لإدارة المعلومات الصحية بالهيئة. يجب أن يكون لدى المنشأة عملية مراجعة وتقييم دورية لكفاءة الموظفين والموارد الأخرى بما في ذلك موردي الخدمة.

4.24.4. يجب على الجهة مراجعة الدورات التدريبية والتوعوية بشكل دوري لتعكس تشريعات وقوانين الدولة المستحدثة والمتطلبات التنظيمية للهيئة.

4.25. عدم الإمتثال:

4.25.1. على الجميع مراعاة أحكام التشريعات السارية على مستوى الدولة والإمارة، والسياسات والأنظمة المعتمدة أو السارية لدى الهيئة وأية تعليمات أو توجيهات صادرة من السلطة المختصة بهذا الشأن، وحيث أن عدم الامتثال أو الالتزام يعرض المخالف لمساءلة قانونية وفقا لأحكام التشريعات السارية[2].

4.25.2. يجب على المنشآت الإبلاغ عن جميع الانتهاكات المتعلقة بمشاركة البيانات والمعلومات الصحية إلى الهيئة من خلال البريد الإلكتروني: datacompliance@dha.gov.ae في غضون 24-48 ساعة.

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

[2] قانون اتحادي رقم 4 لسنة 2016 بشأن المسوولية الطبية

5. Reference

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: ICT Health Law

5.2. Resolution No. (2) of 2017 Approving the Policies Document on Classification, Dissemination, Exchange, and Protection of Data in the Emirate of Dubai. Available on: Resolution No. (2) of 2017

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

5.4. UAE Data Protection Law. Available on: UAE Data Protection Law

5.5. Federal Ministerial Decision No 51 of 2021 Cases Allowing the Storage and Transfer of Medical Data and Information Out of the UAE. Available on: Federal Ministerial Decision No 51 of 2021

5.6. Federal Decree Law No. 34 of 2021 on Combatting Rumours and Cybercrimes. Available on: UAE Cybercrime Law

5.7. Ministerial Decision no. (51) of 2021 concerning the health data and information which may be stored or transferred outside the country. Available on: Ministerial Decision no. (51) of 2021

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: Federal Law No. (5) Of year 2012

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

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

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

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: Law No. (13) of 2021

5.14. Dubai Health Authority Nabidh policies and standards. Available on: Nabidh policies and standards

5.15. Dubai Health Authority Policy for Use of Artificial Intelligence in the Healthcare in the Emirate of Dubai. Available on: Use of Artificial Intelligence in the Healthcare

5.16. Dubai Health Authority Policy for Health Information assets classification. Available on : Policy for Health Information assets classification

5.17. Dubai Health Authority Policy for Health Data Protection and Confidentiality. Available

on: Policy for Health Data Protection and Confidentiality

5.18. Dubai Health Authority Policy for Health Data Quality. Available on: Policy for Health Data Quality

5.19. Dubai Health Authority Policy for Health Information Assets Management. Available on: Health Information Assets Management Policy

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

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

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

5.23. Requirements for an Information Security Management System (ISMS), ISO 270001. Available on: https:// www.iso.org/ isoiec-27001-information-security.html

5.24. Health Insurance Portability and Accountability Act. Available on: Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule

5.25. DHA guideline for patient consent. Available on: DHA Patient Consent

5.26. NHS Data Protection, Access to Information and Information Sharing Policy. Available on: NHS Information Sharing Policy